

## **Building a National IoT Plan: Policy Recommendations and the Case of Brazil**

In 2016, the Nasdaq Educational Foundation awarded the Columbia University School of International and Public Affairs (SIPA) a multi-year grant to support initiatives at the intersection of digital entrepreneurship and public policy. Over the past three years, SIPA has undertaken new research, introduced new pedagogy, launched student venture competitions, and convened policy forums that have engaged scholars across Columbia University as well as entrepreneurs and leaders from both the public and private sectors. New research has covered three broad areas: Cities & Innovation; Digital Innovation & Entrepreneurial Solutions; and Emerging Global Digital Policy. Specific topics have included global education technology; cryptocurrencies and the new technologies of money; the urban innovation environment, with a focus on New York City; government measures to support the digital economy in Brazil, Shenzhen, China, and India; and entrepreneurship focused on addressing misinformation.

---

With special thanks to the Nasdaq Educational Foundation for its support  
of SIPA's Entrepreneurship and Policy Initiative



## Building a National IoT Plan: Policy Recommendations and the Case of Brazil

Ronaldo Lemos, Caio Mario da Silva Pereira Neto, Mateus Piva Adami, Daniel Tinoco Douek, Renata Borges La Guardia, Carolina Milani Marchiori Mesquita, Marcus Vinicius de Abreu Schimitd, Amanda Moreira Kraft, Manuela Oliveira Camargo, Felipe Moreira de Carvalho, Natalia Langenegger, Ramon Alberto dos Santos, Philippe Pessoa Sundfeld, Olivia Bonan Costa, Marina Regina Arvigo, Ellen Stocco Smole Franco, Ana Luiza Stella Santos, Rodrigo Bernardi Bracale, Luis Fernando Braga Amorim, Nataly Fernandes dos Santos

This work serves as a comprehensive survey of the landscape of the Internet of Things and the burgeoning role of regulation in this field, offering insights to other developing countries. Lemos finalized this work while at SIPA.

This is a translation of a work originally written and published in Portuguese and published in the United States and in English with the help of Columbia University's School of International and Public Affairs and the Entrepreneurship & Policy Initiative.

### AUTHORS

**Ronaldo Lemos** is an internationally respected Brazilian academic and lawyer specialized in technology. Lemos is a visiting professor at Columbia University's School for International and Public Affairs. He is a co-founder and director of the Institute for Technology & Society of Rio de Janeiro ([itsrio.org](http://itsrio.org)). Lemos' academic qualifications include a J.D., University of Sao Paulo Law School, a Master of Laws degree, Harvard Law School, and a Doctor of Laws degree, University of Sao Paulo. He is a board member of various organizations, including the Mozilla Foundation, and Access Now. He is also a member of the "Young Global Leaders" community with the World Economic Forum. Lemos was one of the creators of Brazil's Internet Law (Marco Civil da internet), enacted in April 2014, creating a comprehensive set of rights for the internet in Brazil, including freedom of speech, privacy and net neutrality. In 2011, Lemos joined the Center for Information Technology Policy at Princeton University as a visiting fellow. In July 2013, Lemos joined the MIT Media Lab as a visiting scholar. Lemos has received the Prix Ars Electronica Golden Nica in the category of digital communities. He writes weekly to Folha de Sao Paulo, the biggest national newspaper in Brazil, and has contributed to a number of other publications, including Foreign Affairs and Bravo!

**Caio Mario da Silva Pereira Neto** is a partner of Pereira Neto | Macedo's Antitrust and Regulation teams. He is bachelor in Law at the University of São Paulo (USP), and holds Masters and Doctorate degrees from Yale Law School. He is a Professor at Fundação Getúlio Vargas Law School and is currently a visiting professor at King's College London. Caio is the author of several articles, published in Brazil and abroad and he has spoken widely in national and international forums on antitrust and regulation. His antitrust practice includes cartel and abuse of dominance investigations, merger review and compliance, with large experience in multi-jurisdiction matters. His regulatory practice includes advising clients in several regulated sectors (including telecom, transport, energy, health and financial services), regulatory litigation, as well as compliance work. He is also very active on regulatory and antitrust issues in technology industries. He is also recognized among the leading

antitrust and regulatory practitioners in Brazil by Chambers and Partners, Global Competition Review (GCR), Leaders League, Legal 500, among others, and serves as International Director of IBRAC, the Brazilian Antitrust Association. In public service, he held office as Director for Competition at the Secretariat of Economic Law of the Ministry of Justice (SDE). During his term in office, he also integrated governmental committees and working groups in infrastructure sectors under privatization and intense regulatory change.

**Mateus Piva Adami** is a partner of Pereira Neto | Macedo's Regulation team. He is bachelor in Law at Pontifícia Universidade Católica de São Paulo (PUC/SP), holds a Master's degree in Public Law at the University of São Paulo (USP), and is a PhD Candidate at the University of São Paulo (USP) as well. He was an assistant professor of administrative law at Pontifícia Universidade Católica de São Paulo (PUC/SP) and currently is a professor in post graduation courses at Fundação Getúlio Vargas Law School. Mateus has published extensively on matters related to administrative law and economic regulation.

**Daniel Tinoco Douek** is a partner of Pereira Neto | Macedo's Antitrust, Regulation and Media, Technology and Intellectual Property teams. He is bachelor in Law at Universidade Paulista, holds a Masters degree of antitrust law at King's College London and is a specialist in Telecommunications Law and Regulation and State Law from Fundação Getúlio Vargas Law School. Daniel advises a wide range of clients on the most diverse regulatory issues and on the structuration of operations in regulated and non-regulated industries, such as ethanol, railways, seaports, telecommunications, broadcasting and internet.

**Renata Borges La Guardia** is a partner of Pereira Neto | Macedo's Tax team. She is Bachelor in Law at the University of São Paulo (USP), and holds a Doctorate degree at the same institution, besides having an MBA from Fundação Getúlio Vargas. She is a member of the International Fiscal Association-IFA and of other important professional associations. Renata has an extensive expertise in tax law and corporate and tax planning.

**Carolina Milani Marchiori Mesquita** is an associate lawyer of Pereira Neto | Macedo's Regulation team. She is Bachelor in Law at Pontifícia Universidade Católica de São Paulo (PUC/SP). Carolina also studied at Brazilian Society of Public Law's School (SBDP) and attended a short-duration course in Universidad Pablo de Olavide – Spain. She works with emphasis on Public Law and Regulation, having experience in bidding process, public service contracts, regulatory agencies and courts of auditors.

**Marcus Vinicius de Abreu Schmidt** is an associate lawyer of Pereira Neto | Macedo's Regulation team. He is bachelor in Law at Pontifícia Universidade Católica de São Paulo (PUC/SP) and specialist in Economic Law at Fundação Getúlio Vargas Law School. His legal practice is focused on administrative and regulatory law.

**Amanda Moreira Kraft** is an associate lawyer of Pereira Neto | Macedo's Regulation team. She is a bachelor in Law at the Federal University of Paraná (UFPR) and holds a Master's degree in Economic Law at the University of São Paulo (USP). Her legal practice is focused on administrative and regulatory law. Acting mostly in advisory matters, Amanda has experience in various sectors, including power, ports, telecommunications, and railroads.

**Manuela Oliveira Camargo** is an associate lawyer of Pereira Neto | Macedo's Regulation team. She is Bachelor in Law at the University of São Paulo (USP). Her practice has been focused on Regulation and Public Law. She is experienced in both the public and private sectors, having worked as a legal advisor for the Brazilian Presidency's Infrastructure Team Office. She has also worked as a private attorney in other leading Law firms and as a public policy associate for a tech company.

**Felipe Moreira de Carvalho** is an associate lawyer of Pereira Neto | Macedo's Regulation team. He is Bachelor in Law at the University of São Paulo (USP).

**Natalia Langenegger** is an associate lawyer of Pereira Neto | Macedo's Media, Technology and Intellectual Property team. She is Bachelor in Law at Pontifícia Universidade Católica de São Paulo (PUC/SP), holds a Master's degree in Law and Development at Fundação Getúlio Vargas Law School, and is a PhD Candidate at the University of São Paulo (USP). She was a visiting scholar at Tilburg University, Netherlands. She worked on the Secretary of Legislative Affairs of the Brazilian Ministry of Justice, as well as on a well-known technology company. Her legal practice is focused on Media and Intellectual Property, with experience in governmental relations and normative elaboration.

**Ramon Alberto dos Santos** is an associate lawyer of Pereira Neto | Macedo's Media, Technology and Intellectual Property team. He is Bachelor in Law at the State University of Maringá (UEM), and is a PhD Candidate at the University of São Paulo (USP). Before joining the firm, he worked as a Researcher and Teaching Assistant at Fundação Getúlio Vargas Law School. He was one of the managers of Brazil's National Internet of Things (IoT) Plan, commissioned by the Brazilian Development Bank, in partnership with McKinsey & Co, which was published in 2017.

**Philippe Pessoa Sundfeld** is an associate lawyer of Pereira Neto | Macedo's Media, Technology and Intellectual Property team. He is bachelor in Law at the Federal University of Santa Catarina (UFSC), and holds a Master's degree in Intellectual Property Law at King's College London, where he was awarded the Dickson Poon Prize for best dissertation. He has attended the Human Rights in Cybersecurity Workshop by the Global Network of Internet and Society Research Centers, the Summer PhD Program at the Chinese University of Hong Kong, and the WIPO Academy at the World Intellectual Property Organization/University of Geneva. His legal practice focuses on Media and Intellectual Property. He is an invited lecturer at post-graduate courses and is the author of papers in specialized publications.

**Olívia Bonan Costa** is an associate lawyer of Pereira Neto | Macedo's Media, Technology and Intellectual Property team. She is a bachelor in Law at the University of São Paulo (USP).

**Marina Regina Arvigo** is an intern of Pereira Neto | Macedo's Media, Technology and Intellectual Property team. She is a Law student at the University of São Paulo (USP).

**Ellen Stocco Smole Franco** is an associate lawyer of Pereira Neto | Macedo's Tax team. She is bachelor in Law at Pontifícia Universidade Católica de São Paulo (PUC/SP) and has a LL.M in Taxation at Instituto de Ensino e Pesquisa (INSPER) and a specialization degree in International Tax Law at Instituto Brasileiro de Direito Tributário (IBDT). Her tax practice deals with tax consultancy, tax litigation in both administrative and judicial proceedings, tax planning and restructurings. Her practice also includes the taxation of digital economy.

**Ana Luiza Stella Santos** is an associate lawyer of Pereira Neto | Macedo's Tax team. She is bachelor in Law at Universidade Presbiteriana Mackenzie and holds a postgraduate degree in Tax Law at Instituto Brasileiro de Direito Tributário (IBDT). She is a former member of an audit and consulting firm, focused on global tax compliance services. Her practice is focused mostly on tax law advisory and litigation.

**Rodrigo Bernardi Bracale** is an associate lawyer of Pereira Neto | Macedo's Tax team. He is bachelor in Law at Pontifícia Universidade Católica de São Paulo (PUC/SP) and holds a postgraduate degree in Tax Law at Instituto de Ensino e Pesquisa (INSPER). He is a specialist in tax law advisory and litigation.

**Luís Fernando Braga Amorim** is an associate lawyer of Pereira Neto | Macedo's Tax team. He is bachelor in Law at the University of São Paulo (USP). He is a specialist in tax law advisory and litigation.

**Nataly Fernandes dos Santos** is an associate lawyer of Pereira Neto | Macedo's Tax team. She is bachelor in Law at UniFMU and specialist in Tax Management at Fundação Escola de Comércio Álvares Penteado (FECAP).





<b>INTRODUCTION</b>	9
<b>Innovation and entrepreneurship – IoT opportunities</b>	17
<b>Telecommunications Regulation</b>	25
<b>Taxation, fiscal benefits and importation and customs</b>	38
<b>Privacy and Protection of Personal Data</b>	47
<b>Information Security</b>	57
Governance and International Cooperation	57
Brazilian Institutional Arrangement	60
Encouraging Adoption of Security Certification Criteria for Various IoT Components	62
Information Security in Critical Infrastructure	67
Blockchain Technology for Device Certification and Guarantee of Digital Identity	69
<b>Net Neutrality</b>	71
<b>II – ANALYSIS OF PRIORITIZED ENVIRONMENTS</b>	73
<b>Smart Cities</b>	73
<b>Health</b>	117
Regulation of the National Health Surveillance Agency – ANVISA	118
Health Products	119
Regulation of Councils of Medicine	125
The Debate on Privacy	125
<b>Rural Environment</b>	131

## INTRODUCTION

The Internet of Things (“IoT”) is an expression that refers to a whole set of new services and devices that includes at least three fundamental aspects: connectivity, use of sensors or actuators, and computational capacity for data processing and storage. The Internet of Things goes beyond connecting objects to each other; it also gives them the power to process data (thereby making them “smart”).

This development emerges from increased accessibility of already available technologies, which are now being used in mass. For example, a tractor equipped with an IoT device does not simply plow but can also collect data for subsequent analysis. This is done through an app hosted at a data center, which produces reports that allow farmers to make decisions about where and when to plant. In assembly lines, sensors provide data for analysis, which can in turn be used to determine the ideal times to perform equipment maintenance.

Estimates show that the Internet of Things has the potential to add from \$4 to \$11 trillion to the global economy by 2025; in Brazil alone that number could hit between \$50 and \$200 billion. Beyond the economic impact, IoT could lead to extremely significant social gains, such as helping countries achieve United Nations Sustainable Development Goals.

For developing countries such as Brazil, the opportunities offered by the Internet of Things can compensate for shortcomings in infrastructure and services, and can improve innovation, quality of life, productivity, and even the economic complexity of our basket of export products. An example of a high-impact initiative in our cities is implementation of smart public lighting systems. Such systems use monitors and sensors to optimize the use and replacement of public lighting assets, thus enabling the reduction of operational costs for this important service.

Within the emergence of an innovative ecosystem for the Internet of Things, important opportunities are appearing for enhancing the business environment to foster entrepreneurship. The development of an innovative ecosystem for the Internet of Things requires promotion of entrepreneurship, with a particular focus on the role of universities and science and technology institutions in this process.

However, the way in which each country will seize this opportunity will depend on its specific aspirations and strategies. The broader economic, social, political, and legal context of the country should be considered, as well as the local development of information and communication technologies.

For this reason, the National Bank for Economic and Social Development (BNDES), in partnership with the Ministry of Science, Technology, Innovation and Communications (MCTIC), has commissioned this study, “Internet of Things: An Action Plan for Brazil.” This study, mapped by a consortium comprised by McKinsey & Company, the CPqD Foundation, and Pereira Neto | Macedo Law Firm, outlines the local technological and economic challenges related to the topic, as well as how to address legal issues inherent to the development of IoT in Brazil.

The final objective of this technical study is to contribute to the development of a strategic action plan, called the National Plan for the Internet of Things, which is currently being analyzed by

the Brazilian executive branch, so that the country can position itself in terms of public policies in the field of Internet of Things.

One of the main characteristics of this study is its participatory and multisectoral character. It involved the constant participation of several sectors of Brazilian society, through public consultations, events, and working groups. This consultative process helped define priority and strategic actions in order to foment the ecosystem of the Internet of Things in Brazil.

Initial diagnostics: This book aims to present the results of the study on the Internet of Things, but the focus is on local regulatory aspects that can serve as either catalysts or barriers in the development of IoT in Brazil.

First, in recent years Brazil has advanced in the implementation of IoT devices and in providing the necessary infrastructure. For example, in the smart cities environment, there is noteworthy collaboration between the Brazilian Agency for Research and Industrial Innovation (EMBRAPII), the CPqD Foundation, and private partners, enabling the development of smart street lighting solutions for Brazilian cities.

The model developed by this partnership allows municipalities to manage public lighting through smart and connected infrastructure, which in the future may include other functionalities, such as vehicle and pedestrian traffic monitoring. It can also aggregate real-time detection of gunshots, with detailed information on the precise area of the incident, the number of subjects involved, number of shots fired, and even the caliber and type of firearm used, allowing for swifter response from safety authorities.

Meanwhile, on fields and farms, the use of drones, automated machines, and sensors for agricultural production has created new possibilities for productivity, and above all, agriculture based on data analysis. The Internet of Things will help Brazil's already highly competitive agribusiness sector to become more efficient and to reach even higher international standards.

Second, there was a need to reconsider certain aspects of Brazilian legislation and reorganize institutional arrangements: possible changes in telecommunications regulation, the establishment of rules and institutions to deal with information security challenges, the creation of legislation for the protection of personal data by private initiative and the government, and taxation matters and other issues related to import and customs clearance.

Throughout this project, telecommunications regulation was the subject of heated debate. Among the aspects evaluated were the appropriateness of the telecommunications services and obligations imposed by sector regulation on service providers, as these were designed for traditional telecommunication companies offering services directed at users (e.g., requirements for quality of service), and not for machine-to-machine (M2M) communication systems.

Another important consideration is the need to issue a standard that is capable of dealing with the complexity and nuances of personal data, one offering legal certainty for this unprecedented change in society. With the proliferation of new Internet-connected devices capable of storing, collecting, and processing a significant amount of data, there has been a recurrent concern about the legitimate uses of data and the vulnerabilities of the generated databases. There

is also a need for a regulatory entity capable of presenting specific technical opinions and guidance on unified and homogeneous compliance with the rules on personal data protection.

Areas of investigation: After meetings with government actors and other interested entities, the consortium determined that the legal analysis developed within the scope of this study on the Internet of Things would be divided into two main stages of analysis. The first step evaluated horizontal regulatory issues, extending to sectors that may benefit from the implementation of IoT devices: telecommunications, taxation, privacy, and information security. The second step analyzed vertical regulatory issues for sectors previously selected with the support of the Brazilian government: smart cities, health, and the rural environment.

The chapters in this book deal with each of the identified horizontal and vertical issues in order to present the current scenario of regulation (or deregulation), as well as a synthesis of the main potentialities and challenges in question. We intend to offer best practices for the Brazilian Internet of Things sector and to help Brazilian public and private entities achieve better results in areas such as urban mobility, precision agriculture, health, information security, privacy, telecommunications, personal data protection, connected infrastructure, and taxation. Additionally, the study presents several other topics from a legal and regulatory point of view.

Chapter Content: In addition to these introductory notes and a brief conclusion, the information is contained in seven chapters. In Chapter 1, we present some important considerations related to the possibility that the Internet of Things brings to foster innovation and entrepreneurship in developing countries, especially in Brazil.

Chapter 2 examines rules related to telecommunications, given that the applications of the Internet of Things, featuring some kind of connectivity, directly interface with this sector. We deal with the main challenges within Brazilian telecommunications legislation for the efficient implementation of IoT technologies, such as requirements for traditional telecommunications services that provide services directly to users, which are therefore inappropriate for machine-to-machine communication (M2M).

Another challenge concerns incentives to improve the infrastructure of telecommunications networks. Such networks are necessary to access the Internet in Brazil. Therefore, infrastructure improvement is essential for the development of the Internet of Things in Brazil. This study shows that improvements are needed not just in telecommunications infrastructure. Investment in capacity and territorial reach of Internet access services for proper connectivity of the devices also essential.

The study describes possible alternatives to the use of radiofrequency spectrum through these new technologies, such as the use of idle bands in the radiofrequency spectrum and the provision of IoT solutions by means of radiofrequency equipment. The importance of fomenting design for IoT technologies, as it relates to tax exemption for equipment classified as M2M, is discussed.

Given the hybrid nature of IoT solutions, which can range from the importation of components to the domestic sale of devices to services such as software licensing, Chapter 3 deals with issues involving entities in the Brazilian federation (union, states, municipalities) that tax certain services; the accumulation of tributes that may incur high tax burdens; and the difficulty in

approving changes to the tax system by legislative bodies. In addition to describing the challenges encountered by the IoT ecosystem in relation to taxes on income and consumption, we present some existing tax benefits in Brazil that could potentially foster the tech industry. An example is the "The Good Law," which provides benefits for companies investing in research and development of technological innovation, and the Manaus Free Trade Zone, an area of free trade for imports and exports in northern Brazil.

This third chapter also analyzes the imports and customs clearance process in Brazil. It discusses activities of the entities responsible for issuing standardization and regulatory rules, such as the National Institute of Metrology, Quality and Technology (INMETRO) and the Brazilian Association of Technical Regulations, which can play a relevant role in ensuring the interoperability of IoT devices

Chapter 4 discusses issues regarding the privacy and personal data protection of individuals who directly or indirectly use Internet of Things solutions. It includes an overview of the current legislation and regulations in Brazil that address this issue, including the right to privacy as established in the Brazilian Federal Constitution, consumer and telecommunications regulation, the advent of the Civil Rights Framework for the Internet (known in Brazil as the MCI), and its regulatory Decree, which are standards that introduced a microsystem in the Brazilian legal framework to protect personal data on the Internet.

The chapter shows that one of the challenges in the development of a national IoT ecosystem is the adequacy of this legal framework to face issues inherent in new technologies, especially through the issuing of a general law for personal data protection and the existence of a regulatory body capable of ensuring compliance with existing standards and issuing technical opinions on the subject. The institution or designation of such authority should consider the country's political and institutional context, grounded, for example, in the public resources and the organizational capacity of the involved sectors. It should be capable of establishing effective participation, in a true multi-stakeholder movement.

Faced with the expansion of vulnerabilities in networks and the "open borders" nature of information security incidents, Chapter 5 discusses the adoption of measures related to cybersecurity by both public and private initiatives, based on models of international cooperation. This chapter discusses the possibility of Brazil joining the Convention on Cybercrime in Budapest and engagement with Agreements on Mutual Protection and Exchange of Classified Information, a strategy already underway in Brazil. Adherence to these agreements could generate partnerships with countries where there is interest, sophistication, and updates on information security.

At the national level, developers of IoT applications are encouraged to adopt protective measures for information security, either by incorporating voluntary device certification mechanisms or by complying with minimum security criteria in critical infrastructures. We believe that a certification system based on voluntary self-assessment, without the existence of legal obligations for members, has the potential to create a culture of transparency, by providing information to the user and encouraging the acceptance of high-level safety standards by private entities.

Chapter 6 presents an analysis of the importance of net neutrality for the development of IoT, concluding that the rule currently in effect in Brazil does not constitute a barrier for the development of new business models or the implementation of specific services. Possible cybersecurity policies include cooperation from several sectors, such as public power; the private sector; academia; the technical and scientific community; and civil society, among others.

Chapter 7 addresses the offer of improved and more modern services resulting from the use of new machine-to-machine (M2M) technologies. This would include the electricity infrastructure, street lighting, urban mobility, and public safety. Such use of IoT technologies for optimized management of urban public policies has been linked to the still-controversial idea of "smart cities." This use of technological devices in urban areas, capable of collecting data on citizens, monitoring their daily lives, and, in some situations, even identifying them, creates concerns regarding the privacy of the urban population. The chapter begins by presenting the steps authorities must take to enable the collection, processing, storage, and sharing of personal and non-personal data in private and in public environments. For example, authorities should be able to guarantee the security of data collected and the devices used to store it; the use of data for the specific purposes for which it was collected; and the security of anonymization techniques.

Following this, we analyze smart power networks, which incorporate technological information, measurement, and monitoring devices to the infrastructure. This ensures the expansion of multidirectional networks (with energy flowing through the network in different directions, from utilities to consumers, from renewable sources distributed by the network to consumers, from home generation to the network), faster data transmission and quantity, and integration of the energy system with other public services. Our discussion of smart grids will focus on the implementation of smart electric meters in Brazil, devices capable of controlling energy demand through advanced metering infrastructure and consequent regulation by the National Electric Energy Agency (ANEEL). These devices allow for dynamic pricing based on energy availability and instantaneous user demand, in addition to functionalities for monitoring service quality and for identifying anomalies.

Additionally, in this chapter we discuss another aspect of urban public services, the advent of smart public lighting. The replacement of metallic halide lights with light-emitting diode (LED) boards, which are more efficient, can serve as an important inducer for the development of IoT, since it would introduce mechanisms that enable wireless communication with control and communication devices. We discuss the possibilities and obstacles of installing IoT devices in public lighting, including how to regulate the sharing of these assets and the restrictions on the number of fixation points they may have. We identify the ongoing discussion in Brazil of financing of public lighting, in particular the possibility of directing funds from the Contribution for Cost of Public Lighting (COSIP) for the implementation of public-private partnerships, which will be aimed at modernizing lighting in Brazilian cities.

On the topic of mobility, the chapter will discuss how public administration can properly utilize the Internet of Things in traffic control, through the addition of technology to traditional CCTV and radar monitoring, and efficient planning of the municipal transport system. Both the modernization of traffic and urban lighting involves, as we have shown, alignment of federal and municipal regulations with current technological changes. We will also discuss the progressive modernization of public safety mechanisms in Brazilian municipalities, through the adoption of IoT

technologies such as audiovisual equipment and high-definition and sensitivity microphones, new cameras with optical character recognition (OCR) technology, and accurate facial recognition systems. The core of the debate revolves around the need for public administration to consider notions of necessity and proportionality, so that the implementation of technologies with the potential to enhance the fundamental right to safety does not greatly invade the privacy of individuals. We present international initiatives that can serve as a model for Brazilian authorities.

Later in Chapter 7, we conduct a brief analysis of the government's contracting of information and communication technology (ICT) goods and services, which includes hardware, software, and technical assistance services necessary for the execution of public activities. We identify the standards for contracting of these solutions by the federal public administration, which can also serve as parameters for municipal entities in the absence of local regulation. We discuss contracting of a cloud computing service, a relevant example of ICT contracting at the federal level. Also, we address the main impasses for contracting these solutions by public entities, and we systematize ongoing debates about possible adaptation and improvement of existing standards.

In Chapter 8, which discusses healthcare practices, we study regulatory barriers that may negatively affect the development of technologies aimed at monitoring of patient conditions, locating assets within healthcare facilities, and identifying and controlling epidemics. We identify the standards and guidelines that underpin the national health sector, especially those related to the requirement of recording or registering health products at the National Health Surveillance Agency (ANVISA), a public entity responsible for regulating, controlling, and inspecting products and services involving public health risk. IoT equipment may have a therapeutic or diagnostic purpose and, therefore, will be classified as a health product, subject to rules for registration of medical equipment.

Another technological advance in healthcare concerns the use of digital medical records and the exercise of telemedicine (that is, practicing medicine through audiovisual and data communication), both already regulated by the Federal Council of Medicine. As we shall see, the objective of the council in crafting these regulations was to ensure, in addition to professional confidentiality, privacy of health service users. We also highlight concerns about the ability of regulatory entities to keep up with technological advances, since innumerable and diverse IoT applications are being created for the healthcare arena and for processing extremely personal healthcare data.

Finally, in Chapter 9 we deal with the rural environment, addressing issues related to legislation applicable to remotely piloted aircraft systems (RPAS). Current regulations on drones, as these systems are popularly known, may pose a major hindrance to the development of this type of technology when focused on rural activities. This is due to the costs of implementation and the focus on urban use of RPAS, which limits scaling up such technology for rural regions. They have very different conditions from cities, with fewer technical requirements. We also explore the dilemmas that concern connectivity in rural regions, in terms of ownership and protection of data generated through IoT technologies. The aspects of the debate are quite complex, since there are clear differences between the two large groups involved. On the one hand, agricultural producers have advocated for greater protection of data generated from rural technologies, while private initiative

in agricultural inputs and technologies takes the stance that seeks more freedom in the use of rural data.

In conclusion, we will present the main regulatory issues related to the Internet of Things in Brazil in order to provide a global view in this project, presenting the various challenges and complexities for development of the IoT around the world.



## 1 Innovation and entrepreneurship – IoT opportunities

Brazil currently ranks as number 60 among the 63 nations compared in the World Competitiveness Yearbook of 2018. The study compares the performance of 63 countries, based on more than 340 criteria that measure different aspects of competitiveness. Sadly, Brazil stands behind both in terms of competitiveness and in global indexes of innovation, in both public and private initiatives.

It is precisely in this context that the Internet of Things (IoT) can become an important element to increase innovative entrepreneurship in Brazil, contributing positively to the increase of productivity and efficiency, as well as the creation of new markets and new incentives for the private sector.

Innovation and entrepreneurship are important mechanisms for economic development. If applied correctly, they can promote employment and social welfare. To promote the knowledge economy under the Schumpeter framework of "creative destruction" the producer's efforts is relevant. That is to say, the first step towards the emergence of new knowledge and new assets is the strengthening of the role of the entrepreneur and the facilitation of the circulation of credit in the market, essential for innovative efforts.

An entrepreneurial activity can take many forms, mainly due to the changing role of small enterprises in recent years and depending on the institutional context and level of economic development. Jovanic describes the phenomenon of small businesses assuming an increasingly relevant role, surpassing its importance in the last 70 years. Moreover, Acs and Varga developed a study that found that both business activity and agglomeration have a positive and statistically significant effect on economic development.

The entrepreneurial environment varies according to the volume of demand and opportunities, being "marked by interdependencies between economic development and institutions, which affect other characteristics such as the quality of governance, access to capital and other resources and the perceptions of entrepreneurs". This means that each country creates a different terrain for entrepreneurial activity that may differ according to the institution's functioning and to how financial transactions are done within its territory. The link between these elements is crucial to understanding economic development and the importance that IoT assumes.

IoT faces a positive scenario filled with opportunities. Considering the economic specificities, the estimate of global economic impact corresponds to more than US\$ 11 trillion till 2025. In a survey conducted by Accenture, it is estimated that the share of the digital economy in Brazil's GDP will jump from the current 21.3% to 24.3% in 2020 and will be worth about US\$ 446 billion (R\$ 1.83 trillion).

The impact of this phenomenon has been linked to the concept, still under construction, of the fourth industrial revolution. At the end of the eighteenth century, the first revolution was marked by the instrumentalization of water and steam to move machines in England. The second, which began in the mid-nineteenth century, came with the use of electric energy in the mass

production of consumer goods. The third was initiated in the middle of the last century and concerns the use of the Internet and other information and communication technologies (ICTs). The so-called "fourth industrial revolution", in turn, would have started at the turn of this century and has been built from the digital revolution. It is essentially characterized by a ubiquitous and mobile Internet, by sensors and devices that increasingly become cheaper and smaller and by the development of artificial intelligence.

This is the scenario where the Internet of Things grow. IoT is revolutionizing and connecting the world while quantifying and measuring it through devices that can be classified in three categories: (i) wearable devices, (ii) smart home devices, and (iii) machine-to-machine ("M2M") devices. Wearables are those devices that people carry on them and that usually connect to smartphones via Bluetooth, such as smartwatches and fitness bands. Smart home devices use low power wireless communication and the home router. At last, M2M devices are characterized for being directly connected to the cellular network or new networks (such as LPWAN) and acting without human direct interference.

These new technologies can be useful or useless. Useless products tend to weaken the market through features that look attractive due to marketing strategies, but do not improve or benefit people or companies lives. Examples of this type of technology are the egg minder, that just inform how many eggs are left in the refrigerator, and the automatic curtains, which make the product more expensive, without making it more useful. On the other hand, useful technologies are those that we are going to explain in this chapter. They usually concern welfare, security and data privacy.

The evolution of the Internet of Things and its increasing use will lead to the creation of new business models, services and products, and may even substantially change the relationship between producer and consumer. In this line of reasoning, integrating services at the core of industrial, technological, commercial and investment policies seems to be a fundamental step towards increasing industrial competitiveness, entrepreneurship and innovation in a country.

Porter defines competitiveness according to country economic development, pointing out that countries may get stuck between factor-driven and investment-driven or between investment-driven and innovation-driven stages, which constitute the three main stages of a competitive market. The factor-driven stage is the most sensitive one, since it leaves the economy sensitive to world economic cycles, commodity price trends and exchange rate fluctuations. It is marked by high rates of non-agricultural self-employment and by technology-importing. In the investment-driven stage, efficiency is the main concern on large markets, since competitiveness start to grow. The economy continues to be vulnerable, but not to financial crises, as it relies on foreign capital flows and sector-specific demand shocks. In this phase, the workforce moves from a self-employment situation to an employment one. The third stage is conquered when countries recognize the importance of entrepreneurial activity in innovation. It demands public and private investments, higher education, improved capital market and regulatory system beneficial to technological development. In order to Brazil achieve this third stage, it is necessary to improve the environmental market conditions to encourage entrepreneurship.

In the meantime, the difficulties for those planning to undertake or invest in IoT today in Brazil are many, ranging from the lack of a favorable ecosystem (adequate devices and equipment, regulation and connectivity) to the threat of hacking. Yet it seems that managing the volume of information of connected devices is the main challenge to the infrastructure.

In 2015, Industry National Confederation of Brazil developed a study with 100 executive leaders about the level of innovation in the country. When asked the question, 54% of them answered that innovation level was "low" and 8% answered that it was "very low". However, 57% of the companies said that they expected to increase their investment in innovation and the Federal Government, through its development banks, has offered credit lines to small, medium and large entrepreneurs willing to invest in innovation. Within the references in innovation, the executives mentioned the United States, Germany, South Korea, Japan and China, highlighting the investment in education.

In this context, starting in 2017, the Brazilian government has initiated a series of initiatives, including working groups and public consultations, with the purpose of proposing specific policies and regulations aiming to extract all the potential of this IoT scenario. The importance of this type of activity is in the development of a set of projects that is capable of attending to innovation and entrepreneurship, characteristic of IoT, and at the same time protecting fundamental rights of citizens. In other words, the state must approve regulations that protect individual rights, while also creating efficient markets and fostering national innovation.

Nowadays, the IoT market is ruled by big organisations that detain a great amount of capital. They have concentrated research, investment and viability of the IoT so far. However, studies point that the software market is not ruled by these organisations, but by small business that represent up to 93% of the market. This framework seems propitious to the development of other small enterprises with creative and innovative potential, in order to better apply the technologies developed by large companies. In spite of the difficulties to be an entrepreneur, such as heavy regulation and operational costs, we are living in a changing market with new regulations and new incentives.

In 2017, the Securities and Exchange Commission (CVM) has implemented the Normative Instruction n° 588 that regulates investment through equity crowdfunding and ameliorates start-ups scenario. Moreover, pursuant Resolution n° 4.656 of 2018, institutions and fintechs may offer credit services without the mediation of a bank, enhancing peer-to-peer lending, which was impossible until then. It is in this context that we must highlight the promotion of start-ups in Brazil, which face good and unexplored market conditions.

Within the scope of government, the benefits of IoT have been used for greater efficiency of public management. From the use of integrated technologies and massive data processing, more effective solutions to problems such as pollution, congestion, crime, productive efficiency, among others have been identified and implemented. In Brazil, there are already examples of IoT applications in this context, as we shall see, and these experiences tend to increase.

In December 2016, BNDES and the Ministry of Science, Technology, Innovations and Communications (MCTIC) signed a technical cooperation agreement to elaborate the National

Internet of Things Plan in Brazil, which will define the measures to be taken to promote the Internet of Things as a model of development for various sectors. Through a public call, the consortium that includes the National Council for Scientific and Technological Development (CPqD), the law firm Pereira Neto Macedo and the consultancy McKinsey presented to the MCTIC a technical study proposal to offer the first subsidies for the Plan, which was accepted.

In the early stages of the technical study, an Action Plan Report was published containing a selection of key criteria for vertical and horizontal prioritization. Several initiatives were organized in four horizontal categories: (i) human capital; (ii) innovation and international insertion; (iii) connectivity and interoperability infrastructure; and (iv) regulatory framework, security and privacy. For each horizontal, specific objectives were defined. Vertical analysis refers to cities, health, basic industries, houses, stores, factories, offices and administrative environments, logistics, vehicles and rural areas. Finally, the four vertical areas defined as priorities for Brazil's actions through IoT were: (i) smart cities; (ii) health; (iii) rural area and; (iv) industry.

Brazilian business community has also recognized the potential of IoT. In a recent survey by Accenture with more than 1,400 executives revealed that they were very aware of the opportunities that IoT can offer and highlighted the three main benefits expected: increasing employee productivity, cutting costs and optimization in the use of assets. A better consumer experience has also been listed as one of the expected benefits. It was also identified great potential for the introduction of solutions / products associated with technologies incorporated by IoT in the development of the services sector, which represents an important part of the Brazilian economy. Therefore, the enthusiasm with IoT's economic potential has promoted a strong investment in this area, for example, in the so-called "industrial IoT" sector, geared toward infrastructure solutions such as smart cities, cargo tracking, precision agriculture, and energy and asset management.

These new IoT investment fronts stem from the positive profit outlook for the sector. Just as an example, it is worth mentioning the research carried out by Cisco which estimates that the Internet of Things can add 352 billion dollars to the Brazilian economy by the end of 2022. Forecasts like this show a potential for innovation and investment that attracts both governments and companies that are developing concrete initiatives.

In the cities environment, the number of small players, or even startups, is very significant: 35% of all suppliers have less than 10 employees and another 35% have more than 100 employees. Although the performance of smaller players represents dynamism and attractiveness in this vertical, the high number brings uncertainty about the development of this scenario in the next five or ten years. In Rio de Janeiro, for example, the region of Praça Mauá was chosen for the transformation of the Social and Urban Innovation Program of a multinational connectivity company. The program features 15 intelligent solutions developed by the company and technology startups, and its main IoT solutions include initiatives such as air quality monitoring and better management of sewers, public lighting, water leakage in pipes and noise.

In Uberlândia, Minas Gerais, the neighborhood of Granja Marileusa, was created by private initiative to receive IoT applications. With energy and data network infrastructure, the neighborhood has more than 95 homes with video monitoring and fiber optics installed. Equipped

with dumps with volume sensors, the neighborhood still gave rise to a technological micro pole and has a space of coworking to attract innovative companies.

In Ceará, in Croatá city, the project Smart City Laguna, also carried out by private initiative, aims to be the first intelligent social city on the planet. Created in 2011, it builds on the pillars of social inclusion, urban planning, environment and technology. With the construction of government-supported houses, the neighborhood provides free use of technologies to obtain information and therefore to monitor resources such as water and energy. The project already has private partners for the provision of smart meters, intelligent public lighting, free Wi-Fi signal and security systems.

One concern mentioned in the technical study carried out by the consortium involved in the National IoT Plan concerns the collection, storage and sharing of personal data, offering potential privacy risks. Thus, with regard to the collection of personal data in the urban environment made through IoT solutions by the public sector, it is advised that it must be done with anonymizing techniques, whenever possible, through robust criteria of encryption, among others. It is also crucial to adopt measures capable of inhibiting the illegal use of data and the surveillance of the individual by the State and private agents.

In the area of health, IoT applications can also bring great benefits, since this technology can contribute both to improve the quality of life of the population and to increase the efficiency of health units, counterbalancing the global challenge of increasing costs with health. Across the world, the potential economic gain that IoT can bring to health, by 2025, is estimated at between US\$0.2 and US\$1.6 trillion, and in Brazil, the estimate ranges from US\$5 to US\$39 billion. In both cases, the estimated impact range is large, as there are many steps and barriers for new technologies to be widely adopted in this sector. By comparison, the impact represents between 3% and 21% of total health expenditure in Brazil in 2014, according to data from the World Bank.

There are several concrete experiences of IoT in health in Brazil: from the fight against infections in hospital environment to the reduction of wastage. Some companies have also developed solutions to perform diagnostics in a decentralized manner, avoiding the costs related to the transportation of biological materials to perform exams.

The health area is open to the development of devices, sensors, embedded systems, energy storage methods, and also to connectivity tools. It is an area with strong potential in issues related to the network infrastructure and development of IoT solutions. On the other hand, there are several barriers to the development and adoption of IoT in health in Brazil: regulatory issues, the challenge of privacy of the clinical data of the people (sensitive personal data), connectivity in remote areas, among others factors.

In Brazil, the health sector has relevant players that offer IoT solutions. Aside from the major medical device manufacturing companies, the number of IoT-related startups in health has also increased. Research shows that at least 85 institutions among companies, universities and institutes of science and technology already provide some kind of solution for health. In addition to these institutions, another 31 reported that they intended to offer solutions to the health market in 2017, and 149 reported that they are studying the development of solutions.

In the rural environment, the applications of IoT can benefit the producers of the various Brazilian production chains. The different applications of IoT to the field allow the monitoring of climatic conditions, the growth of the plantation, the performance of agricultural machinery, and the detailed monitoring of animal health and irrigation of the fields. These applications have the potential to bring important gains in productivity and cost reduction, increasing the competitiveness of Brazilian agricultural products in the international scenario.

A study conducted by the McKinsey Global Institute measured the global impact potential of IoT in the rural environment. In this area, the estimated potential economic gain that IoT can bring is US\$ 61 to US\$ 362 billion in 2025. According to the Brazilian technical study led by consultancy McKinsey, IoT is expected to move US\$ 132 billion in the Brazilian economy by 2025. The initiatives can benefit more than 70 sectors in the country. In the field of agribusiness, the investment in IoT can improve the productivity and the quality of the sector, besides increasing the relevance of Brazil in the world trade of agricultural products.

The offer of IoT solutions for agriculture was mainly made by global companies of this branch. However, many Brazilian startups have also been emerging and expanding internationally, offering various IoT solutions tailored to the tropical climate. The Brazilian market has been a pulsating and propitious environment for the creation of new businesses in agriculture technology (AgTech). A mapping of the national market shows the diversity of companies that already offer IoT solutions to the field. Technology companies offer a wide range of solutions ranging from data integration through big data and advanced analytics to recommendations, to animal monitoring and agricultural production by sensors. Companies provide solutions across the value chain, from input production to specific software and hardware development and trading solutions. Nevertheless, to be fully realized the development of IoT in this area, it is necessary to overcome relevant structural barriers related mainly to the lack of connectivity infrastructure, the difficulties of fostering innovation and the low professionalization of the workforce.

Technology companies are increasingly interested in developing IoT solutions aimed at creating mechanisms by which demanders and suppliers can interact and align efforts. This type of interaction between applicants, suppliers and support entities, also known as "innovation network", has a great appeal for rural vertical as well as for other prioritized verticals, and has been deepened in the study of the Brazilian National Plan for IoT. Within the industry, the development and incorporation of new technologies have led to changes in business models and design, engineering and production processes. Rapid scanning, widespread use of sensors, the creation of integrated control and automation solutions, and the analysis of massive data are some characteristics of modern industries.

The Brazilian National Plan for IoT selected four representative sectors in the industrial area: automotive, textile, mining, and oil and gas. The first two are linked to manufacturing and the last two linked to industrial process. The automotive industry is leading technology in terms of manufacturing and has expanded strongly in recent years. Since the first half of the twentieth century, government policies have stimulated the development of this sector in Brazil, which is now much more used than other modes of transportation. The textile sector has an important installed base, however with smaller companies and a pulverized production chain. It is a sector that combines IoT technologies, artificial intelligence, robotics and automation, while giving the customer

the possibility to choose what they want to use and the design of the products. The oil and gas sector, in turn, has a robust production chain, with large operating companies and new paradigms of offshore production. It is, at the same time, an essential part for the support of the entire IoT application chain and fertile terrain for digital transformation. Mining is a mature and globally competitive sector that can make use of IoT to reduce environmental impacts and gain greater control and efficiency in the process. All these sectors have in common the fact that they already have initiatives in progress related to IoT, which corroborates the study in these segments .

The four prioritized environments (cities, health, rural and industry) rely on their particularities and specific technologies. However, according to the Plan, four points stand out as being of common necessity. The first relates to machine learning, which allows increased processing capacity, analysis and efficiency. The second deals with the use of algorithms, especially through deep learning, to maximize machine learning technologies. The third seeks to deal with big data, whose organization will be required to handle the huge volume of data circulating in IoT applications. Lastly, the fourth instrument concerns the use of computers in a decentralized way in order to reduce transmission delays, network intermittency and operational costs to the maximum extent possible.

With so many challenges, companies are pursuing more ambitious strategies to increase efficiency in order to ensure viability and growth. Digital technologies play a critical role in this movement. Recent technological advances have the potential to usher in a great wave of increased productivity and performance, but only if companies leverage the right technologies to sustain their business strategies.

There are many possible applications of IoT in the industry and through entrepreneurship, from remote asset tracking to predictive maintenance, through inventory management to control solutions. However, the development is still uneven between industries and the rate of adoption is low in Brazil. All sectors can benefit from the development and adoption of IoT. The realization of experimental projects makes possible the learning and the greater acceptance of the new technologies in the different sectors. Expanding this process and enabling the development of more complex and sophisticated technologies in the various segments will also depend on the incentive to cooperation between the public and private sectors, as well as between companies, their suppliers, service and equipment demanders, universities and research centers. The public sector alone should not develop products and IoT technologies alone, but rather create policies that encourage others to do so, including a strong incentive for entrepreneurship and public-private partnerships.

Even in its nascent stages, the Internet of Things is already transforming our world. Keeping us more connected and aware, the IoT's full potential has yet to be realized. With various social organizations already mobilizing support and resources through IoT networks, it has been shown that by using technology, social entrepreneurship has been able to thrive unlike ever before.

It will be necessary to invest time and financial resources in an industry still devoid of: infrastructure consistent with the amount of Internet access and information generated; standards and languages for the interoperability of IoT systems; frameworks, such as regulations and specific laws; security to collect and store information without infringing on people's privacy and exposing

strategic business secrets. All this at a time when the Brazilian economy undergoes a recession that is long, credit restriction and low consumption. There are already mobilizations of large private organizations and the Brazilian government to overcome the challenges cited and generate an environment conducive to the development of IoT in the Country. The entrepreneur's role at this time is to work for the creation, adoption and development of a culture of innovation in companies, universities and government, doing his part in forming a favorable ecosystem for the implementation and growth of the Internet of Things.

In the following chapters we will present the regulatory analysis that were made during the technical study organized by the BNDES and the MCTIC, and which tries to pave the way for this new wave of innovation and entrepreneurship in Brazil.



## 2 Telecommunications Regulation

From the perspective of telecommunications sector regulation, connectivity is a particularly relevant issue in the development of the IoT market. This is because connectivity –between people, devices and people and between devices – is an essential feature of any telecommunication service. Considering that IoT applications have some type of connectivity and, therefore, direct interface with the telecommunications sector, it is necessary to first identify the potential obstacles that may arise from this intersection.

In the case of IoT applications, the connectivity provided by a telecommunications service may be contracted: (i) directly by the user of the IoT application (e.g. from a Personal Mobile Service operator – “PMS”), and they will become a user of the telecommunications service; (ii) directly from a partner telecommunications provider, as an input to the provision of the IoT application, in which the telecommunications service is embedded; or (iii) offered directly by the IoT provider itself based on its own telecommunications network.

In the first case, there are no great regulatory challenges to overcome, considering that connectivity will be provided by a telecommunications operator contracted directly by the user in a common service provision relationship – which may be the most common arrangement for IoT applications. In the last two cases, however, connectivity would be embedded in the IoT application itself as offered to the client, which may lead to some regulatory discussions:

- a. in the second case – i.e. connectivity contracted by an IoT solution provider from a telecommunications operator – questions may arise regarding possible unauthorized resale of the telecommunications service to the IoT user;
- b. in the third case – i.e. connectivity offered by the IoT provider itself – the offer will depend on the current regulatory regime, on obtaining a specific grant for the operation of the telecommunications service, even if this telecommunications network is for the IoT provider’s own use.

Classification of an activity as a telecommunications service raises a series of regulatory requirements ranging from: previous need to obtain a grant for the service provision, eventual authorization for the use of radiofrequency, licensing of stations, certification and approval of equipment, payment of sectorial charges and compliance to quality obligations, among others.

The regulation itself does in fact establish, under some circumstances, the exemption or simplification of one or more of these regulatory obligations. However, these exemptions or regulatory disparities may not be enough to cover the range of IoT applications and to promote their development in the country.

This is partially explained by the way in which the General Telecommunications Law (“GTL”), Law no. 9.472/1997, and ANATEL regulations were designed, that is, based on a telecommunications service provision model to users (individual or business entity), and, therefore, based on direct relationships with telecommunications service providers (i.e. connectivity).

IoT applications, however, may depend on a series of models that depart from more typical service relationships. For example, the lack of human interaction in the majority of IoT applications render inappropriate certain burdens imposed by the sector regulation, more typically directed at traditional telecommunication services provided directly to the user (e.g. quality standards and requirements), and not machine-to-machine (“M2M”) communication.

This is relevant even in situations in which IoT depends only on a connection that is already available to the user (e.g. residential connection for a security application), as well as for general sector bottlenecks (e.g. infrastructure deficiencies and lack of mass access to broadband services). This may also hinder the creation of an environment favorable for IoT development in Brazil.

These and other concerns will be described, in order to identify means for the adequate development of the IoT market in Brazil.

### *Main Contribution Points*

#### 2.1. Change in the concept of M2M

To begin, it is necessary to revisit the definition of M2M communications, an essential concept for many IoT functionalities. This is evidenced by a series of contributions collected during the Public Hearing on the Internet of Things, indicating the need to revisit the machine-to-machine (“M2M”) concept or machine-to-machine communication present in Decree no. 8.234 of May 2, 2014.<sup>i-ii</sup>

The above Decree states that is considered M2M communication systems, in order to justify tax incentives as provided for in Law no. 12.715/2012, those systems without human intervention, using telecommunication networks to transmit data to remote applications to meet objectives that involve monitoring, measuring and controlling a device, the environment to which it belongs, or the data system to which it is connected, through the utilized networks.

However, considering that many devices depend and will depend on some level of user interaction for their adequate functioning, questions emerge. The use of the “human intervention” concept is considered insufficient, since these IoT applications have various degrees of interaction with their users, which makes them difficult to categorize.

Some initiatives seeking to revise the law aim to offer greater discretion to ANATEL.<sup>iii</sup> Such initiatives include removing “human intervention” as the central point of the “machine-to-machine communication systems” concept.<sup>iv</sup>

This difficulty has been previously faced in other jurisdictions, including Germany and Canada.

In Germany, the decision was made to define M2M communications as those that are “predominantly automatized”. Although not typical, human intervention would be admitted in a limited extent that would not declassify it as a M2M communication.<sup>v</sup> In Canada, M2M communication would be identified in devices that communicate automatically without the need for “direct and conscious” human interaction.<sup>vi</sup>

It is worth noting that international examples utilized undetermined legal concepts – i.e. “predominance” or “direct and conscious” human intervention –, which demand caution in interpretation of the law.

In any event, the definition in Brazil must offer legal certainty, so that no market distortions are created, especially where there is the establishment of fiscal or regulatory disparities in favor of IoT devices.

A replacement of Bill no. 7.406/2014 is currently before Congress. Article 21 alters the current wording of Article 38 of Law no. 12.715/2012. According to the wording of the replacement text, the concept of M2M would be defined in the law itself and would encompass “communication devices for data transmission and remote applications with the objective of monitoring, measuring and controlling the device itself or its surrounding environment or the data system to which it is connected through these networks”. Although creating greater legal certainty is admirable, the concept proposed by the replacement text may be interpreted as too limiting for many IoT innovations. That is because, in addition to being vague, its definition in law may limit future changes in the concept.

Therefore, the German example, based on the idea of “predominance”, generally offers more flexibility for existing and potential future business models, especially compared to the “indirect and unconscious” concept as proposed by Canadian law.

Therefore, if considering the need to change the concept of M2M communication in Brazil, the recommendation is to consider proposing a change to Decree no. 8.234 of May 2, 2014 to introduce a concept that includes the rationale of automatization “predominance” and which would lead ANATEL to promote a detailed regulation that prevents distortions.

## 2.2. Telecommunications Infrastructure

Given that using the telecommunications network infrastructure to access the Internet is a premise for development of IoT, actions for expanding investment in Brazilian access networks and telecommunication transportation will be explored.

We will adopt the following premise: considering the connection of thousands of devices to Brazilian telecommunication networks and the consequent exponential growth of data traffic, it is essential to create incentives for new investments for expansion of access to those networks.

However, policies for access and widespread availability of telecommunication services are expected to face legal challenges. In this regard, the challenge is sufficiently understood and sufficient solutions are being developed.

In terms of resources to enable expanded access to telecommunication networks, there are three priority measures:

- a) Bill no. 79/2016 suggests solutions to two concerns: (i) changing the telecommunication services from the concession model to the authorization model; and (ii) addressing the reversibility of assets used to provide granted services.<sup>vii</sup>

According to this proposal to change the General Telecommunications Law, changing the model would require payment of an amount to be determined by the Agency, for which the funds could be used to expand broadband in Brazil.

Although the proposal from Bill no. 79/2016 has not yet been approved, the fact remains that resources generated could be a relevant source of investment for expanding Internet access.

- b) Additionally, there should be discussion regarding application of resources from the Fund for Universal Access to Telecommunication Services (known as “FUST”) for expansion of broadband Internet access.<sup>viii</sup> Although the fund is the only instrument for universal access to telecommunication services, its resources have barely been used for such.<sup>ix</sup> Considering that FUST has many resources and an efficient financing system, it would be important to use it as a mean to promote IoT solutions.
- c) Finally, there is the option of expanding access to telecommunication services using resources from Conduct Adjustment Agreements signed by ANATEL and operators to replace penalties with obligations. Through these agreements, the Agency can replace financial penalties with mandatory investments and other benefits to users – which would also result in the expanded distribution of access to telecommunication services.

Beyond measures to enable financial resources for expansion of Internet access, an appropriate public policy to expand the capacity of networks to access and transport telecommunication service is important. According to information obtained by the Consortium, these matters will be addressed by the future National Connectivity Plan, which was subjected to a public consultation in 2017.<sup>x</sup>

In this way, compatibility between the National IoT Plan and the National Connectivity Plan is essential, and for other eventual public policies for expanded access of telecommunication service, as the success of the first depends on the effectiveness of the second.

### **2.3. Aspects Related to Concessions for Providing Telecommunication Services**

The eventual need to obtain concessions to provide telecommunication services is of special importance for the development of the IoT market.

IoT applications require contracting or using a telecommunication service as support provided through the concession of a Multimedia Communication Service (“MCS”), a Personal Mobile Service (“PMS”) or a Private Limited Service (“PLS”). Since the enactment of ANATEL Resolution no. 680/2017, MCS and PLS services provided by networks that exclusively use guided transmission media and/or radiofrequency equipment do not need a concession to provide telecommunication services, and must only comply with other regulatory obligations.

We must address some additional points referring to (i) the offer of connectivity embedded in IoT and the need for a previous concession to provide telecommunication services; (ii) aspects related to PLS to provide IoT applications; (iii) regulatory limitations in exploring Mobile Virtual Network Operators (MVNO); and (iv) numbering resources and permanent international roaming.

i) Embedded Connectivity

The connectivity embedded in devices utilized by IoT solutions may generate questions about regulations, since the distinction between telecommunication services and value-added services (“VAS”) may not be clear in different IoT solution business models, especially in situations where there is an integrated offer of both services.

In the current regulatory framework, whenever an IoT application provider offers, along with VAS, a functionality that qualifies as telecommunication service provision, a previous concession from the regulatory agency is necessary, except when explicitly provided for by law and by the sector regulation.

A series of questions arise from this scenario: is any type of telecommunication service functionality (e.g. voice communication) applicable to sector regulation? Does contracting of a telecommunication service by an IoT provider which later offers a different service to the final user mean that the service is considered a telecommunications service provider? Should there be a contract signed between the IoT application user and the telecommunication service operator – or even a contract that also includes the IoT application provider itself? These questions tend to inhibit certain IoT solutions or even undermine new and more efficient business models.

Considering the current regulation and the position of ANATEL according to no. 399/2010/PVCPR/PVCP, as well as the competence of ANATEL to deliberate on the interpretation of telecommunication legislation and omitted cases (Art. 16, XVI of GTL), this Regulatory Agency must evaluate the possibility of issuing a precedent on this subject to offer legal certainty to market agents who are interested in providing IoT applications.

This hypothesis aims to offer more legal certainty to IoT business models in which the embedded connectivity is contracted by the IoT solution provider from a telecommunications operator as a service, in which case this could help avoid eventual discussions over a possible unauthorized resale of telecommunication services to the IoT user.

In cases where embedded connectivity is offered by the IoT provider, through its own telecommunication network (PMS or PLS) or through a shared network (MVNO), there may be the need for a specific concession to operate telecommunication services, even when the telecommunication network is for the IoT provider’s own use. The following sections will address regulatory aspects related to concessions for PLS and MVNO as alternatives to some IoT business models.

ii) Aspects Related to Private Limited Services (PLS) for Provision of IoT Applications

PLS is regulated by ANATEL Resolution no. 617 of May 19, 2013. It establishes the need for a PLS concession to provide telecommunication services, in restricted mode, in favor of self-execution or provided to determined user groups selected by the provider.<sup>xi</sup>

This PLS model became more relevant with ANATEL Resolution no. 680/2017, adding Article 5-A to ANATEL Resolution no. 617/2013, which exempts the need for PLS concession when telecommunications exploration and support networks are exclusively through guided transmission media and/or radiofrequency equipment. This was previously allowed only for specific categories of the latter.<sup>xii</sup>

Although ANATEL has never determined limits of expression “for determined user groups”, it does not generate any legal uncertainty to agents interested in offering IoT applications to a pre-determined group of users under the limits of PLS. This is exemplified by a statement from ANATEL, item no. 1706/2017/SEI/ORLE/SOR-ANATEL<sup>xiii</sup> regarding a business model adopted by a telecommunications company focused on IoT that characterized itself as such:

Referring to the communication sent by you on May 19 of 2017, part of case no. 53500.057940/2017-52, in which you presented a business model regarding the offer of IoT services through the use of radiofrequency equipment operating in the 902-907.5 MHz, 915-928 MHz bands, to clarify and inform as follows.

Radiocommunication stations using equipment, apparatus or device that use 902-907.5 MHz, 915-928 MHz bands for different means and in which emissions produce an electromagnetic field within the limits established in the Regulation for Radio Wave Equipment approved by Resolution no. 680 of June 27 of 2017, are exempt from licensing for installation and operation.

Additionally, the company has reported that it is a service for a determined user group, which characterizes it as a Private Limited Service – PLS. Given that the PLS will be provided only for use of radiofrequency equipment, an authorization from ANATEL is exempted, and the company must communicate its activities, as provided by Art. 5-A of the Private Limited Service Regulation, transcribed below:

Art. 5-A. PLS providers with support telecommunication networks that exclusively use guided transmission media and/or radiofrequency equipment are exempt.

Paragraph 1. The provider exercising the aforementioned exemption must communicate the start of its activities in advance to the Agency through ANATEL’s electronic system. [Emphasis added]

Paragraph 2. The provider using the exemption must update its registration data annually, before January 31, through ANATEL’s electronic system.

Paragraph 3. This exemption does not exempt the provider from compliance with conditions, requirements and duties established in the legislation and regulation.

Communication must be done through the Mosaico System, according to guidelines on the following page: <http://www.anatel.gov.br/setorregulado/servico-limitado-privado>.

Therefore, considering what is presented in the document (SEI no. 1478325), it is confirmed that the proposed operation does not depend on previous concession from ANATEL, under the terms of the Radio Wave Equipment Regulation, approved by Resolution no. 680/2017, of the Private Limited Service Regulation, approved by Resolution no. 617/2013, and of articles 131 2<sup>nd</sup> Paragraph, and 163, 2<sup>nd</sup> Paragraph, II, of the General Telecommunications Law – Law no. 9.472/1997.

PLS is therefore an important tool for telecommunication service provision focused on supporting of IoT applications, currently with unlimited use within some IoT business models, as determined by the Agency.

The fact that in the current PLS model may challenge data communication between network devices and the public network is something to consider, as the interconnection of telecommunication services of restricted interest to the public network is prohibited by the Telecommunication Services Regulation. Although the interconnection may occur through user access, this type of connection would entail a cost increase for the IoT provider.

Therefore, if IoT devices which are offered based on a telecommunication services of restricted interest, with the need to connect to the public network, the responsible operator of IoT solutions must then (i) become an operator of telecommunication services of collective interest or (ii) as a user, contract a telecommunication services operator of collective interest. This situation deserves attention, as it can generate legal uncertainty and undermine some IoT business models.

iii) Mobile Virtual Network Operator - MVNO

MVNO concessions may also be employed in connectivity through the sharing of mobile networks with mobile service providers in IoT, and it is currently provided for by specific regulation in two categories: Authorized MVNO and Accredited MVNO.

It should be noted that current standards for configuring MVNO are found in ANATEL Resolution no. 550 of November 22, 2010, which has occasionally been modified since its publication to expand the adoption of the model<sup>xiv</sup> - which has been the subject of incentive by the regulatory body.<sup>xv</sup> Perhaps this regulation should be revised, considering the context in which it was created may no longer be aligned with the aim of expanding IoT in Brazil.

An MVNO is strictly prohibited from having a representation contract with more than one provider in a determined registration area, which obliges the virtual operator to use one single network to support its services (a regulatory limitation that may preclude business models that require national coverage) or to adopt the authorized category, which is more complex and costly. The revision of this regulation to allow the representation of more than one operator could include the MVNO using the best available network in a determined time and place, benefitting its users.

Reflecting on Brazilian MVNO regulation or potential small changes to ANATEL Resolution no. 550 of November 22, 2010 could contribute to a more favorable environment for the development of the IoT market. ANATEL is understood to have an important role in communicating to the market regarding MVNO as an important access solution.

iv) Permanent International Roaming

Another aspect that deserves attention is the use of foreign numbering resources. As determined by ANATEL, smart devices used in Brazil must use a Brazilian number resource to connect to a network and use telecommunication services in the country.

This requirement to use national numbers raises a problem in the use of foreign devices imported to Brazil. Currently, this has been addressed by changing the device's SIM card. By installing a Brazilian SIM card with a national number, a device can connect to a network and use telecommunication services.

However, when considering an expanded scenario in which smart devices do not allow for chip exchanges, new technologies offer alternative solutions to this problem, often proving to be more efficient.

An example of such new technology is the e-SIM, a chip that is integrated to the device. Although the card cannot be replaced, the device can be remotely programmed, allowing the device with this technology to substitute the numbering resource through an over-the-air update.

This shows that it is possible to change the numbering of a device through remote reprogramming without having to physically change the SIM card, which would solve matters involving: (i) imported devices; and (ii) devices that don't allow for physical chip substitution – e.g. for safety reasons.

The e-SIM is an alternative to the national numbering issue in imported devices, making business models that use numbering from foreign providers irrelevant.

Furthermore, ANATEL has previously discussed the impossibility of using chips that do not allow operator transferability.<sup>xvi</sup> This obligation originates from ANATEL text no. 8 of March 19, 2010, which guarantees this right to customers.<sup>xvii</sup> During that era, a device with an integrated chip that prevented free choice of an operator did in fact deter usage. However, the advances in e-SIM configurations have resolved this issue.<sup>xviii</sup>

In this sense, the e-SIM presents an alternative to the need for permanent international roaming to allow the development of specific IoT business models in Brazil. Many functionalities enabled by IoT will involve the circulation of devices from foreign countries connected to foreign providers. ANATEL still has demonstrated that it is not in agreement with this type of model and considers permanent international roaming as irregular.<sup>xix</sup>

With the e-SIM being remotely reprogrammable, agents would be allowed to change operators without purchasing a new SIM. This would facilitate the operator and would render unnecessary permanent international roaming.<sup>xx</sup>

Considering the current stage of ANATEL regulations, as well as the growing development of IoT related functionalities, there are three possible scenarios for implementation:



- a) Regulation via total prohibition, considering that ANATEL has not yet issued regulation makes official the prohibition of the practice, a fundamental action to establish more legal certainty to market players.
- b) In a completely opposite route, ANATEL could adopt a position of total liberation for use of permanent roaming in Brazil, which would require extensive studies, as well as practical matters (e.g. numbering limitation), competitive matters (e.g. inauguration of regulatory parity for Brazilian and foreign operators) and legal matters (e.g. efficiency of the concession system after the flexibilization).
- c) Finally, an intermediate alternative would be to partially liberate the use of permanent roaming only to M2M communication devices. This would demand the implementation of a measure to coordinate the allocation of number blocks that would be previously “reserved” to attend to integrating applications.

The option should consider a strict evaluation of the real impact of permanent roaming on IoT applications in Brazil, considering alternatives to this flexibilization – like the previously mentioned e-SIM or MVNO. This is important to consider, since it involves a consolidated market situation (situation “b”) or the creation of an uneven regulatory measure (situation “c”) – which, although not unprecedented in the sector, nevertheless must be duly substantiated.

With this, the main issues in concession-related matters appear to be addressed.

#### 2.4. Rational Use of the Spectrum

As mentioned in the subsidies document, it is also necessary to address the use of radiofrequency spectrum, a relevant aspect in the context of IoT.

In this case, this would include access radiofrequency to support IoT applications. The focus will be on: (i) the creation of a secondary radiofrequency market; (ii) rules for industrial exploration; (iii) increase of the non-licensed spectrum.

Regarding the first point, there is currently no secondary radiofrequency market, since it is currently impossible to transfer authorization without also transferring the telecommunication service to which it is bound. However, with the aforementioned Bill no. 79/2016, there appears the possibility of changing the General Telecommunications Law, with the possibility of transmitting the use of radiofrequency without that authorization. If the wording is approved, Brazil would appear on the list of countries that allow the secondary spectrum market.<sup>xxi</sup>

From a regulatory point of view, the proposal is considered an interesting measure to ease the rational use of the spectrum, which is expected to grow – therefore balancing the supply-demand equation for this input. In a scenario of free radiofrequency resale, flexibilization of the use of the spectrum could be maximized, different from what currently happens.

Beyond this, it is worth noting that the secondary market is not involved in the possibility of conceding radiofrequency through industrial exploration, currently regulated by ANATEL Resolution no. 671, of November 3, 2016.

The resolution provides an option for a more efficient use of the spectrum, considering that, although it entails the granting of radiofrequency through a series of requirements and observing of adequate procedure, it does provide for cases that do not require prior consent from the Agency (Art. 41, Paragraph 6). It would be important to evaluate, along with the market, if current rules and regulations are appropriate for promoting the efficient use of the spectrum.

Also considering the new regulation of industrial exploration, it would likely be necessary to immediately map the use of licensed spectrum in Brazil, as provided for in Art. 5, I, of ANATEL Resolution no. 671, of November 3, 2016 (periodic confirmation of effective use of radiofrequencies). If it is determined that there is no use of the spectrum by its operator, ANATEL could reasonably evaluate the eventual need to review the applicable regulation or adopt measures to encourage the adoption of this business model.

The aforementioned Resolution shows a need to discuss the reasons for forbidding the grant of radiofrequency for primary use. From a legal point of view, there are no reasons to impede the liberation of this type of grant for uses beyond secondary.

Regarding the third point, from the legal point of view, it is worth noting that the allocation of the spectrum should follow international allocation standards to avoid distortions and incompatibilities between equipment produced in Brazil and in other countries – which would generate a series of losses to services.

## 2.5. Equipment certification and approval

Another area of great importance is the certification and approval of equipment used to provide telecommunication services.

Recently, as mentioned in the text on subsidies, ANATEL revised its requirements for development, aiming at swift development of the IoT market in Brazil.

Beyond the above mentioned impediments, it should be noted that current certification and equipment homologation does not consider information and data security risks, as related to the spread of IoT in the country and the increase of connected devices susceptible to failures and attacks.

The requirement of a minimum safety standard for certification and improvement of equipment could avoid or, at the very least, mitigate such risks. However, some discussions are necessary:

- a) Conflict with the principle of technological neutrality. Depending on the required conditions, the regulatory option could imply exclusion of certain technologies and business models from the market, inhibiting innovation and freedom in contracting.

- b) Diversity of applications. There are countless means of applying devices to IoT solutions – and to others that may emerge in the future. This makes it difficult to create one standard that covers all possible applications.
- c) Different degrees of criticality. The use of various equipment may occur in a more or less critical manner, for which a security requirement may also be more or less necessary. While for less sensitive applications, the demand for stricter standards may not be necessary, the same would not apply for more critical applications (e.g. fire detectors, hospital devices, etc.).
- d) Technical limitations. Extremely restrictive devices (e.g. sensors) for example, are not capable of cryptography, not even of light cryptography.
- e) Technological evolution. It may render obsolete security criteria that is sufficient for protection of users and the network. Likewise, more modern security technologies may be created in the future.
- f) Expertise. Expertise is needed to deal with this matter. Currently, ANATEL is the best-prepared organ to evaluate these criteria, but even the Agency has its limitations in handling an infinite number of new requests for approval/certification of IoT devices. In fact, issues addressed by ANATEL are more related to radiofrequency and to the users' physical safety, and do not involve other security aspects such as cryptography, for example.

Additionally, even the creation of distinct standards for applications or application groups is difficult. This is because it would be impossible to identify a priori the functions that manufactured devices would assume after their commercialization.

## 2.6. Quality Requirements

Having addressed matters related to the certification and approval of equipment, we now move to another extremely relevant discussion for IoT in Brazil: minimum quality requirements in service provision.

Meeting Quality Management Regulations (QMR) indices for different uses of IoT may be a significant barrier for IoT development.<sup>xxii</sup> Since there is no current differentiation for functionalities of devices that use telecommunication services, all PMS and MCS must assume the same level of regulatory onus.<sup>xxiii</sup>

Speed is currently the only aspect subject to larger commercial variations, while other characteristics, such as latency, are subject to minimum quality requirements. This restriction may not be able to provide greater freedom to operators that provide telecommunication services or offer IoT applications.<sup>xxiv</sup>

Considering that greater freedom among operators to offer plans appropriate for IoT applications – e.g. with higher bidirectional latency – may lower the costs of the activity, QMRs may be an obstacle to this objective.

This is very much related to the relevance of developing a clear and modern M2M communication concept. Beyond enabling the reconfiguration of FISTEL, this measure would also allow the prompt adjustment of quality regulations so that M2M devices may be partially or fully exempt (within a logic of identifying minimum standards that would be considered essential).

If ANATEL considers a change in the content of these QMRs to be potentially negative for consumers, the flexibilization of quality indices for M2M for legal entities is proposed as a possible solution. Along with this measure, procedures for conflict resolution already present in ANATEL should be used to establish greater legal certainty.

In any event, the regulatory agency seems to be aware of the need to review the quality parameters for telecommunication services, as in Public Hearing no. 29/2017, to gather contributions for the new Telecommunication Service Quality Regulation.<sup>xxv</sup> It is essential that ANATEL consider the need for changes to foster IoT applications.

## 2.7. Debate on FISTEL Exemption

Finally, the exemption of M2M communication systems is a sensitive matter for the development of the IoT universe in Brazil – since the ARPU (Average Revenue Per User) per connection becomes extremely low.<sup>xxvi-xxvii</sup>

FISTEL's obligation to collect, from stations used in telecommunication service provisions, represents a relevant onus. It is a fact that the costs involved have already been partially reduced, particularly due to Art. 38 of Law no. 12.715 of September 17, 2012: the inspection tax per chip to be collected from FISTEL fell from R\$ 26.83 to R\$ 5.86. However, this was insufficient to solve the problem.

Other than increased demand for smart solutions, the fact that many functionalities involving FISTEL have lower market values than connection fees must be considered – e.g. telecommunication station. Initially, this may render the product, and its utilization by the general population, inviable.

As a proposal to promote smart devices, Bill no. 7.656/2017 – previously mentioned and currently before Congress– proposes a change to Law no. 12.715 of September 17, 2012 to establish complete tax exemption for inspection of the installment and functioning of telecommunication service mobile stations, considered as M2M communication.<sup>xxviii</sup>

It should be noted here that ANATEL has already responded to Bill no. 7.656/2017, having emphasized the relevance of the proposal. According to the Agency:

“the regulatory impact of the legislative proposal is insignificant. Such an aspect was raised within the strategic project of revaluation of the station concession and licensing model, having verified that, in 2016, the revenue from the collection of the Functioning Inspection Tax (FIT) from ‘machine-to-machine’ stations was R\$7,806,787.90 [...], while the revenue from the FIT collected from other types of stations was R\$2,424,589,731.00 [...]. Therefore, ‘machine-to-machine’ stations correspond to only 0.32% of revenue from the mentioned tax, the same proportion in relation to the

CFPB (Contribution to Foster Public Broadcast) and to the CFCI (Contribution to Foster the Cinematographic Industry)”<sup>xxix</sup> [Emphasis added]

The ANATEL statement is extremely relevant, as it disproves any argument that exemption would be unfeasible based on revenue amounts.

The path to exemption may diverge from the idea of changing regulations as proposed by Bill no. 7.656/2017. ANATEL itself considers the possibility of a change in the GTL, in Art. 162, to exclude M2M stations from licensing obligations, which would consequently remove incidence of all taxes and contributions.<sup>xxx</sup>

It is essential to understand the need to reduce costs to expand devices that use M2M communication, and a measure must be implemented.

### 3 Taxation, fiscal benefits and importation and customs

#### 3.1. Taxation

The National Tax System, as will be shown below, can be problematic in terms of promotion of new technologies, including the development of IoT, due to the overlapping of activities, from importation of components, domestic sales of devices, usage of telecommunication services,<sup>xxxix</sup> realization of value-added services<sup>xxxix</sup> and services of other kinds (licenses<sup>xxxix</sup> and software development).

Given the hybrid nature of IoT, many issues can arise, especially since (i) there is an accumulation of consumption taxes that generate fairly high tax burdens, with multiple incurrence of taxes on consumption,<sup>xxxix</sup> which, in turn, are cumulative; (ii) there are numerous uncertainties regarding ability to tax certain services, due to the lack of clarity of what communication services are (subject to Tax on Transactions of Goods and Services of Interstate and Intermunicipal Transportation and Communication - " ICMS " - a state tax) and are not (subject to "Tax on Services of Any Nature " - ISS, municipal tax); and (iii) approval of any change in the system is extremely complex, such that the current tax system is still defined by the Federal Constitution of 1988 and anchored in a National Tax Code of 1966.

Added to this is the need to comply with an extensive list of additional obligations required by the Federal Government, 27 States and 5,500 municipalities, which creates a great drain on taxpayer time and resources. According to the World Bank study Doing Business (2017)<sup>xxxix</sup> a company in Brazil must spend 2,038<sup>xxxix</sup> hours per year to pay taxes and meet other obligations. Brazil is ranked 181 among 190 countries, behind countries like Mexico, Colombia and the rest of Latin America.

The situation makes development of IoT unattractive in Brazil. For this reason, simplification of the tax system is needed, through the development of fiscal policy that minimizes the above-mentioned issues, and introduces fiscal incentives similar to the M2M incentive, capable of fostering technological development.

##### a. Characteristics of the IoT Environment that Affect Taxation

Technological innovations have given rise to the so-called digital economy,<sup>xxxix</sup> which affects the commercialization of goods and the offering of services, through new business models. These changes promoted by digital technologies directly affect the national and international tax system, as they break with the traditionally known concepts of goods and services. The IoT, in this context, gives rise to many issues already facing technological development, as well as presenting new problems, demonstrating the fragility of the current tax system. The most relevant aspects from a taxation perspective are the following, as they directly affect the parameters that are traditionally used to classify activities and selection of taxable persons. Specifically, these aspects are: mobility of services provided; the intensive use of sensors connected to devices (as it generates significant data transmission); volatility and innovation; and diversity of the business model.

## b. Impact of IoT on Income Tax

The IoT environment is incompatible with concepts used to establish tax jurisdiction: residence, permanent establishment or source, both in Brazilian domestic legislation and in the Treaties agreed upon under the OECD Model Convention. This is because such concepts require some kind of physical presence from taxpayers and beneficiaries, either through an installation or a representative. This physical presence characteristic is often inconsistent with IoT.<sup>xxxviii</sup>

In addition, the IoT system requires an in-depth analysis of how gains produced by the data and information collected should be taxed.

One of the most relevant features of IoT, as already noted, is the specific ability to collect, process and share data through a system connected to multiple devices, sensors and cloud components. The IoT system enable effectively the formation of a database of technology companies in an exponential way.

Therefore, the data collected in the IoT environment is essential in the digital economy, and its valuation is a complex task, since such data can be obtained directly from users (through registry) or from observations (access records, location and date) and data destination can be variable, that is, it can be sold directly to third parties or be used for new products and services. For no other reason, the data are considered as the blood life of digital economy<sup>xxxix</sup>.

And in this context, the income tax should serve as one of the tools to tax the wealth earned by a company because of the development and exploitation of activities in a country. The problem is that the current income tax rules are very much anchored in concepts related to physical presence and are not able to capture the nature and the production factors of the digital economy. For this reason, technology companies are profiting from the exploitation of data obtained from users worldwide, but do not tax the wealth generated in the countries where profits originated, due to the inadequacy of current tax regulations.

Therefore, what would be the impact of this data on the transfer pricing rules and profit allocation of the permanent establishment? For all these reasons, establishing value and taxing for data is not a simple task.

Additionally, in this regard, the IoT environment generates new business models, which may involve simultaneous delivery of telecommunication services, and products and services of other natures. With this, there are several simultaneous forms of monetization, which may impact taxation income on items such as advertising revenue, acquisition or leasing of digital content, or on applications or sales of content, products and services, software licensing, and data.

With this range of possibilities, questions emerge about how to characterize these operations and the income produced in applying domestic legislation and Treaties. At both a national and international level, income taxation may vary according to the nature of income, e.g., payments to beneficiaries abroad are subject to withholding tax at the rate of 15% to 25%; on the other hand, the rate is 15% for remittances in general and 25% for services in general. Royalties and

technical services, on the other hand, are subject to a 15% tax rate and an additional 10% contribution (known as "CIDE" in Brazil). As a result, it becomes difficult to characterize both these transactions and the income produced for tax purposes.

c. Impact of IoT for Taxation on Consumption

In relation to the consumption tax, it should be noted that IoT activities are developed in a system that involves (i) supply of the merchandise (the device); which will (ii) connect to the Internet, through telecommunications networks; for (iii) transmission of data and information monitored by said devices.

This broad range of activities involved in the IoT system makes identification of the end-activity and the identification of the applicable tax regime. In Brazil, this distinction of activities becomes particularly relevant because the supply of goods and communication services are subject to the incidence of ICMS [VAT tax], whose taxing power belong to the States, while the provision of services in general, including VAS, are taxed by the ISS, whose taxing power belong to local governments.

This type of discussion about the nature of the activities carried out, which is reflected in conflicts of taxing power between States and Municipalities, is frequent, for example, in the controversies surrounding the taxation of (i.) Internet access providers; (ii.) softwares; (iii.) insertion of advertising material in digital media.

In this context, the IoT system can further aggravate the jurisdictional conflict between States and Municipalities, as IoT-related activities present scenarios more complex than the current situation. Depending on how IoT activities evolve, communication services may be used only as a means for other utilities. If connectivity is offered to users, this would be considered a communication service, with consequent application of the ICMS.

In addition, the IoT environment allows the development of transactions at a global level through the integration of companies and users through a command center that can be located geographically far from where the operations are carried out and where the users and / or suppliers are located. Add to this the fact that users can move constantly and cross borders of municipalities, states and countries,

This feature directly affects issues related to the origin and destination of the activity, which are important criteria in establishing tax jurisdiction of the ISS and ICMS. The taxing power of the ICMS between States is determined according to the origin and destination of the goods, whereas, in the ISS, the taxing power is directly related to the location of the establishment or, in specific situations, to the place where the services are actually rendered. The peculiar conditions of the IoT environment make it difficult to identify the relevant territorial elements to delimit jurisdiction for the collection of taxes, leading to conflicts of jurisdictions.

Imagine a hypothesis in which a person can have access to data services from any locality, so that a predetermined destination cannot be specified. In this case, which entity should collect taxes?



Currently, given the Brazilian tax system, the state that should collect tax cannot be precisely determined. Questions also arise if importing this type of service from a foreign company, abstractly speaking, directly by the individual as final consumer, to determine whether there is a taxable event or not. If it is, another question arises: who would be responsible for the tax and which state would collect it?

The dilemma does not end there. The same type of problem arises within the scope of service operations which, depending on their type, are subject to the ISS. Therefore, given the abstract aspect inherent in IoT services, this subject will likely trigger discussions on competence and location for purposes of levying and collecting taxes.

#### d. Example of the Types of Conflict

An example of a conflict that incorporates the above issues might be, for example, a company offering real-time vehicle monitoring. Such a service would allow operators to obtain broad information about fleet vehicles, such as location, speed, engine operations, whether the merchandise contained within is properly cooled, and so on. In addition, functions would include automatic temperature adjustment of the chamber and a speed lock.

For this activity to be developed, the use of a telecommunication service is needed, initially provided by an operator, as well as a value-added service that collects vehicle data. The data is processed, and commands can be issued to control the conditions of the vehicle. Here we should note that the provider does not necessarily need to be located in Brazil. The provider may service national territory, while the servers may be located abroad, in which the concept of residence for tax purposes would not be applicable. On the other hand, could the chips installed in the vehicles be understood as permanent establishment, thereby applying the residence concept for tax purposes?

Likewise, identification of the location of the user and the service is complex, since tracking can be remote and the vehicle is in constant movement. In this case, which State or Municipality would have the jurisdiction to tax this activity? In fact, the very nature of this service is called into question; initially it would be a VAS, but once it makes communication via a telecommunications network, it effectively provides a communication service. Which holds more weight? Who is consuming the collected data? And, finally, how is it being economically leveraged?

As already shown, the IoT environment could be impacted by existing conflicts and debates within the scope of national taxation. In addition, the service sector provided by IoT is very recent in Brazil, which may lead to the emergence of other tax issues important to IoT development in the country.

### **3.2. Fiscal benefits**

There already exist some tax benefits that could theoretically foster industry focused on IoT.

It is important, however, to clarify that the benefits mentioned here are potential ones, since some issues, still to be defined, may influence the realization of these benefits, such as (a) the manner in which products are marketed in the IoT environment; (b) the need to import parts and components, for which there may or may not be similar products in Brazil; (c.) the production of products being entirely abroad or in national territory, etc.

This information is of extreme importance in determining the utilization of current benefits and is essential for effective utilization by companies working in the IoT environment in Brazil. Each of the current tax benefits are outlined below.

a. Operating Profits Benefits

The Operating Profits benefit, instituted by Provisional Measure no. 2.199-14, of August 24, 2001, provides for 75% reduction on income and additional tax calculated based on the exploration profits,<sup>xi</sup> for companies that have the project approved by December 31, 2018, for installation, expansion, modernization or diversification within certain sectors of the economy considered as priorities for regional development in the areas of operation of the Northeast Development Authority (SUDENE) and the Superintendency of Development of the Amazon (SUDAM).<sup>xii</sup>

The aforementioned priority measures were established by Decree No. 4.212, dated 4.26.2002, and 4.123, dated April 26, 2002, respectively. In the IoT environment, those that would be applicable in theory would be those aimed at the manufacturing industry in the following groups: (a.) electronics; (b.) mechatronics; (c.) computing; and (d.) the components industry (microelectronics).

However, to utilize the benefit, the legal entity must have a project registered and approved by December 31, 2018. The benefit can be ten years, starting from the calendar year following the start of the operation. The Ministry of National Integration must certify these operations.

In addition to the abovementioned reduction, Provisional Measure No. 2.199-14/2001 also offered income tax and additional tax exemption, calculated based on exploration profit for legal entities that manufacture machinery, equipment, instruments and devices based on digital technology, directed at the digital inclusion program.

Research and Development in Technological Innovation

Legal entities that invest in researching and developing technological innovation should take advantage of the benefits provided for under Law No. 11.196 of November 21, 2005 (the "The Good Law"). It should be noted, however, that the benefits provided by the Good Law can only be exercised if the innovation results in a new product or manufacturing process, as well as the aggregation of new functionalities or characteristics of the product or process, which implies incremental improvements and effective gains in quality or productivity, resulting in greater competitiveness in the market.

In sum, the tax benefits applicable in this case imply a Corporate Income Tax Reduction (IRPJ), Revenue Tax Withheld at the Source (IRRF), Social Contributions on Net Profits(CSSL), Tax on Industrialized Products (IPI), as follows: (a) possibility of deduction in the calculation bases of the

IRPJ and CSLL, with a value of 60% to 80% of expenditures made for research and the development of technological innovation; (b) 50% reduction of IPI on machines, equipment, apparatus and instruments for technological development; (c) accelerated depreciation in full, for the purpose of calculating IRPJ and CSLL, in the acquisition of the new products mentioned in (b); (d) accelerated amortization, by deduction as loss or operating expenses, of expenses related to the acquisition of intangible assets classified as deferred assets; and (e.) reduction to zero of the IRRF rate on remittances made abroad for the registration and maintenance of trademarks, patents and cultivars.<sup>xlii</sup>

#### b. Manaus Free Trade Zone

The Manaus Free Zone is a free trade area for imports and exports with special tax incentives,<sup>xliii</sup> established to develop the rural Amazon region, and administered by the Superintendence of the Manaus Free Trade Zone ("SUFRAMA").

This region<sup>xliii</sup> offers tax incentives from the government, state and municipal governments, in addition to other financial incentives<sup>xliv</sup> offered by SUFRAMA for implementing industrial and agricultural/livestock projects under its area of actuation. The benefits offered by SUFRAMA, for the implementation of industrial and agricultural projects in its area of coverage. The benefits are intended for the product and not the project, and the manufacturing company only benefits from them once starting production.

There are several benefits that can be granted to companies that are interested in operating through the Manaus Free Trade Zone. There also exist generic incentives that can be used or adapted to the operations carried out under the scope of the IoT.

Among the roster of existing benefits, there is a reduction of up to 88% of Import Duty (II) on the inputs destined for industrialization, exemption of the Tax on Industrialized Products (IPI) on imports realized through the Manaus Free Trade Zone and resales of industrialized products in the Zone for the entire country, exemption of PIS/PASEP and Cofins (social contribution taxes) in internal operations of the Zone, ICMS Tax Credit on the tax due on existing products (ranging from 55% to 100%), deferral of ICMS on imports of raw materials, among other current benefits.

Also, for companies that produce IT goods according to the Basic Productive Process (known as the "PPB")<sup>xlvi</sup>, investing 5% of gross revenues in research and development activities in the Amazon, there are specific benefits in Import Duty (II) and Tax on Industrialized Products (IPI) exemptions.

#### c. Computer Law

A fiscal benefit was established for companies that develop or produce computer goods and services, or invest in research and development activities in technology located outside the Manaus Free Zone.

Law no. 8.248, of October 23, 1991 (the "Computer Law"), provided for cases of reduction of IPI on computer goods produced in accordance with the PPB, which can be applied throughout the national territory, as well as the Center-West, SUDAM and SUDENE. The IPI reductions in these cases

can vary from 70% to 100%, in the production of, among others, electronic components, electronic inputs, machines, equipment and devices based on digital technology, with functions of collecting, treating, structuring, storing, switching, transmitting, retrieving or presenting information, parts, pieces and hardware for operation, computer programs, machinery, information processing equipment and devices and associated technical documentation (software).

In order to use this benefit, companies producing said goods must invest 5% of their gross revenues annually in research and development activities to be carried out in the Amazon.

Below are the benefits that may not be used in conjunction with those outlined in item (c) above.

d. Ex-tariff

Finally, a potential incentive to be leveraged in the development of the IoT environment is the Ex-tariff. This consists of up to two years of a temporary reduction in the Import Tax on Capital Goods, on Computing and Telecommunications, as well as its parts, pieces and components, that do not have an equivalent produced in Brazil, as written in the Mercosur Common External Tariff (CET).

Currently, this is governed by the Brazilian Chamber of Foreign Trade (known as “CAMEX”) Resolution No. 66, dated August 14, 2014. The interested party must request the Ex-tariff to the Department of Production Development at the Ministry of Development, Industry and Foreign Trade (MDIC), accompanied by catalogue and product descriptions, among others. Following an admission procedure, if all the requirements are fulfilled, a special Ex-tariff is created for the products in the CET subject to reduced rates.

### 3.3. The Process of Importation and Customs Clearance

In further developing these issues, it is important to analyze the process of import and customs clearance in Brazil, which has great importance in the development and expansion of IoT solutions.

In fact, there exist many import rules to be followed and importers must be accredited under different control systems established and managed by the Brazilian Federal Revenue Service and by the Ministry of Development, Industry and Foreign Trade. Therefore, any components and goods intended for importation, and that are necessary for the development of IoT within the country, must also comply with said controls and rules.

In practice, the most common important process issues usually occur in the parameterization phase, which may delay clearance of goods and, consequently, may delay the taxpayer’s intended commercial operations and increase the cost of customs duties. This phase of the import process begins with a preliminary analysis of the documents presented, and depending on this first analysis carried out by customs inspectors, there may be different outcomes.

The deadlines for processing an import, then, depend on the parameterization channel for which it was submitted for Import Declaration. The legislation only provides for deadlines for imports determined as green and gray channels, and do not provide for yellow and red channels. In the green channel, customs clearance is usually immediate, and in the case of the gray channel, it

may reach up to 180 days (where the merchandise must pass through a procedure called customs conference). As the legislation does not address deadlines for yellow and red parameterization channels, court decisions have determined as reasonable an eight-day average for the Brazilian Federal Revenue Service and customs agencies and intervening subordinates to analyze all paperwork they deem relevant.

As mentioned, depending on the parameters used for determining an importation, there are concerns on the effective timeframe for customs clearance and consequent liberation of merchandise. If an import process does require a more detailed analysis, a parallel administrative procedure may be initiated, whereby the tax authorities will need to review everything they deem necessary to certify that the import is regularized, and only when this parallel process concludes may regular processing of the operation begin.

From a fiscal point of view, key examples of problems in establishing parameters are: (i) cases in which the tax authorities have doubts about the tax classification (according to Mercosur Common Nomenclature) adopted for the merchandise being imported, a fact that may even be reflected in taxation on the operation.

In many of these cases, there exists a specific process to verify the characteristics and nature of the imported good, with a request for an examination and whatever else may be necessary to ensure accurate tax classification; (ii) cases for which tax authorities have doubts about the origin and flow of the goods, or about the prices charged in the transactions (i.e. triangulation hypotheses and fraudulent filings by persons established in other countries, non-observance of transfer pricing rules in transactions among affiliate companies, antidumping frauds affecting national competitiveness, etc.).

As mentioned, there are a number of rules and controls to be observed in the context of the Ministry of Foreign Trade ("COMEX") operations, which involve, taxes not just on importers but on those necessary for the import process to take place (carrier, regulatory agencies, port logistics, dispatchers, Brazilian Federal Revenue Service, Secretary of Foreign Trade, etc.).

In this context, it is worth mentioning that Brazil recently adhered to the WTO Trade Facilitation Agreement, which aims to reduce bureaucratic impacts on imports and exports, to reduce transportation time and costs and the like, among other objectives.

Prior to this, Brazil was already preparing for this new reality, and a single Foreign Trade Portal was created, whose pillars include the integration of stakeholders, the redesign of processes and an investment in information technology. Aligned with this agreement, this portal aims to gradually standardize all COMEX rules and procedures.

Also, as a measure to mitigate bureaucracy in COMEX operations, the Brazilian Authorized Economic Operator Program (known as "OAS") was created in 2015, which according to the Brazilian Federal Revenue Service aims at granting various types of certifications to interested companies. Depending on the level of certification granted, stakeholders will be entitled to a number of benefits in the import flow, such as a reduced percentage of selection channels on import and export, early registration of Import Declaration for maritime shipping, response to tax classification in up to 40 days, participation in seminars and training, among other benefits.



## 4 Privacy and Protection of Personal Data

Privacy and protection of personal data within the Internet of Things ecosystem needs to be considered for reasons beyond its potential to improve the telecommunications regulatory framework.

The increase of devices connected to the Internet and able to store, collect and analyze a significant amount of data has brought an ongoing discussion on the genuine use of data and the vulnerabilities of generated databases. In addition, the formulation of public policies, the efficient and transparent management of government organs and the creation of new business models are all influenced by the exponential growth of analysis based on a great volume of data.

Considering that the development of Internet of Things solutions involves changes in standards of personal data protection and in the complexity and detail of personal data, what is needed is legal certainty in this scenario of major changes in society.

Beyond changing specific standards on personal data protection, a regulatory body is needed to deal with the current challenges of social information – a new authority capable of presenting specific technical opinions on this new environment and managing personal data protection compliance in an integrated and uniform way.

### 4.1. The Need to Create a Privacy and Personal Data Protection Authority

Possible institutional designs for a Personal Data Protection Authority in Brazil will be presented in this section. We start by noting that during the National IoT Plan formulation and public consultation processes, there was a consensus that such a body would be necessary to protect personal data.

To present regulatory possibilities for such an authority in Brazil, we will explore various international experiences. We will briefly describe a number of institutional models in the United States and the European Union; these currently are at the center of global debate on personal data protection. In terms of a South American structure, we will analyze Uruguay's experience.

The Brazilian legal framework on privacy protection shows significant gaps which will be covered by the recent approved General Data Protection Law (LGPD, Law no. 13.709/2018) which will come into effect in 2020. However, the president at the time, Michel Temer, vetoed articles providing the creation of a National Authority on Data Protection and National Council on Privacy and Data Protection under the argument that there was a legislative form non-observance. Therefore, the law was approved without stipulating a competent entity to supervise and promote actions and studies on privacy and data protection. Some problems that were previously detected will persist, such as those resulting from the fact that related standards are simultaneously regulated by multiple entities: SENACON (the National Consumer Secretariat, linked to the Ministry of Justice), the Federal and State Prosecutor's Office, and so on.

The creation of a Personal Data Protection Authority may mitigate this problem. It may also prevent abuses in the collection and handling of Internet users' personal data and in systems of IoT.

Until the LGPD's approval, the legal contours on personal data protection in Brazil were provided mainly by the Internet Framework and by Decree no. 8.711/2016. Although it provides the minimum standards of privacy protection on the Internet, requiring that personal data can only be provided to third parties when users freely express their informed consent (Art. 7<sup>th</sup>, VII), the regulatory framework itself notes the need for a specific standard related to data to be developed in greater detail (art. 3, III).

In order to reduce the legislative gap, the LGPD provides higher standards of privacy and data protection. It is the result of the combination of two Bills (Bill no. 4.060/2012 and Bill no. 5.276/2016) and inspired by the General Data Protection Regulation (GDPR) from the European Union. In spite of having established similar principles and objectives, the final text of the law does not have any specifications regarding the creation of a competent authority.

In a society that is increasingly guided by data analysis,<sup>xlvii</sup> it is an important provision not only for citizens, but also for the private sector and the State itself, since the increase of new devices connected to the Internet and capable of collecting different data, as is the case of IoT technologies, makes database attacks and misuse of personal data increasingly common and compromising. In addition, the managerial capacity of such actors is conditioned on and has been increased through the collection, storage and automated processing of data by elaborate algorithms. The analysis of great volumes of data<sup>xlviii</sup> directly influences the formulation of public policies, the efficient and transparent management of governmental organs and the creation of new business models.<sup>xlix</sup>

In this scenario, the development of solutions for machine-to-machine communication involves specific changes in personal data protection standards and in dealing with the complexity and detail of personal data, in order to assure legal certainty to this new frontier of society, especially considering that the expansion of IoT may increase violations of citizen privacy.

Other than changing and improving specific and current norms on personal data protection, it is necessary to establish a regulatory body capable of presenting specific technical opinions on privacy protection in different market segments and on managing the personal data protection compliance in an integrated and uniform manner.

Existing regulatory models, the main ones being state regulation, co-regulation and self-regulation<sup>i</sup> must be considered in establishing this regulatory body. The model recurrently found in Brazil is state regulation, in which Regulatory Agencies (such ANEEL and ANATEL) concentrate and conduct the organization of a determined market segment.<sup>ii</sup>

On the other hand, self-regulation<sup>iii</sup> is less common. It consists of regulation conducted by market agents themselves and development and implementation of mechanisms for compliance standards.<sup>iiii</sup> In this case, the possibility of imposing penalties differs from police powers, and are applied by the self-regulated community itself. This action presents different results, such as the development of codes of conduct, models for contracts, codes of ethics and certification of quality. Although self-regulation is nothing new, it has been significantly expanding since the emergence of the Internet, and its effectiveness varies according to different factors such as governmental



incentives, the composition and transparency of the development body and the application of the created rules.<sup>liv</sup>

Finally, co-regulation initiatives are defined by the government and private agents sharing responsibilities for activities, such as the formulation of norms and regulatory standards and their enforcement.<sup>lv</sup> This regulation model is expressed in varying ways and degrees, such as governmentally supervised self-regulation or negotiated rulemaking. The intent here is to unite various stakeholders to develop rules that would receive incentives and regulation conducted with state support.<sup>lvi</sup>

Consideration of the local context is essential when deciding upon a regulatory model for personal data protection authority. A blueprint solution replicated in different countries is not recommended, as it cannot consider local government resources, the organizational capacity of the sectors and political will.<sup>lvii</sup>

Studies developed over the past few decades show that the most effective existing Personal Data Protection Authorities rely on different stakeholders (“multistakeholderism”), with real mechanisms for true collaboration with these actors, with high levels of transparency and responsiveness.<sup>lviii,lix</sup> Another key aspect is their competence and actions, such as the commitment to educate the community about personal data protection in Internet usage.

Therefore, the design of the regulating body must consider the local political-institutional context and align with the technical complexity and dynamics of the Internet. Also essential is truly participative decision-making processes, institutional capability to provide parameters of conduct to the market and the ability to inspect for compliance with related legislation.

#### 4.1.1. International Experiences

This section provides a brief description of institutional personal data protection standards in the United States, the European Union and Uruguay. The US and EU regulatory models differ from one another and are of particular interest, as they show how the international community has been dealing with citizens’ personal data protection. Uruguay plays a prominent role in personal data protection in Latin America; personal data protection is considered a human right in the Uruguayan Constitution, and is guided by specific legislation and a government organ.

All three models require consent of the user to collect, handle and use personal data, prescribe transparency obligation requiring the individual to be provided with some basic information, and granted the right to access, rectify and remove data.<sup>lx</sup> However, these models have different roles for the State and the market in regulation and enforcement.<sup>lxi</sup>

In the United States, the State’s role is reduced to standards by sector, and the Judicial Branch is the last resort for conflict resolution. In Europe, the Data Protection Authority is the main actor in standardization and acts on the administrative resolution of conflicts, in order to avoid cases going to court. Similar to the European model, in Uruguay the State has an important role in conducting inspections, as previous registration of databases is required by the protection authority.

In regards to the market, US legislation requires that most practices related to personal data and privacy be defined by the agents themselves through auto-regulation practices through signing of contracts, always subject to judicial approval. On the other hand, the European Union uses mechanisms from the market to encourage adherence to guardianship standards defined in data protection norms. Finally, the Uruguayan system is similar to the European system, as it allows for registration of Codes of Conduct developed by banking and private data associations and entities, under the protection authority, provided it complies with the law.

#### a) European Union

Until 2018, in the European Union, personal data protection was ruled by Directives no. 95/46/CE and no. 2002/58/CE, which was issued from the mid-1990s to the early 2000s by the Parliament and the European Council to standardize the legislation in the Member States.<sup>lxii</sup> The first one is the main regulation for personal data protection in the European judicial system,<sup>lxiii</sup> and the second one addresses the handling of personal data and the protection of privacy in electronic communication.<sup>lxiv</sup>

In January 2012, the European Commission proposed a reform of the current rules for personal data protection, resulting in Regulation no. 2016/679 (General Data Protection Regulation - GDPR) and Directive no. 2016/680. These new rules aim to allow the user to control the collection, handling and use of their personal data and aim to simplify the regulatory environment over the subject. The rules were published in May of 2016 and took effect May of 2018.<sup>lxv</sup>

Specifically, in relation to a personal data protection authority, Article 8 of the Charter of Fundamental Rights of the European Union<sup>lxvi</sup> requires that the personal data protection Authority be an independent organ. The European Data Protection Supervisor (EDPS) is an independent, advisory, supervisory body responsible for assuring that institutions and organs of the European Union respect obligations concerning data protection. Among its responsibilities are the control of personal data handling, advising institutions and bodies of the EU and processing complaints and investigations.

Established by Article 29 of Directive no. 95/46/CE, the Working Group was an independent advisory body for data and privacy protection, formed by representatives of data protection national authorities from the Member States, EDPS and the European Commission. In general, this organ issued recommendations, opinions and other documents.<sup>lxvii</sup> It was substituted by the European Data Protection Board (EDPB)<sup>lxviii</sup> in 2018 under the GDPR. The EDPB is part of EDPS and intends to be the center of the new data protection landscape in EU, issuing guidelines on the interpretation of GDPR concepts and ruling binding decisions<sup>lxix</sup>. At the same time, the European Commission has the role of proposing and enforcing legislation, as well as implementing policies and allocating EU funding, accordingly with EDPB interpretations<sup>lxx</sup>. In addition, there is also a Data Protection Officer, responsible for assuring that the Commission adequately applies the legislation related to personal data protection. In addition to cooperating with the EDPS and informing all departments responsible for personal data collection in the Commission and data subjects of their rights and obligations, the Officer maintains a database with all of the Commission's operations involving personal data.<sup>lxxi</sup> Furthermore, Member States have national data protection authorities working with all mentioned bodies.

Therefore, the EU has a predominantly regulatory model for privacy and personal data protection – given that GDPR determines how personal data is to be protected, and that there are authorities responsible applying it at national and supranational levels - with significant co-regulation indications. An example of co-regulation in the European continent would be binding corporate rules, when European and foreign companies contractually define rules for personal data protection in their transnational exchanges.

#### b) United States

On the other hand, the United States does not have specific and consolidated federal legislation on personal data protection. The matter is presided over by a series of sector-based federal laws and state laws, as well as Codes of Conduct and rules established by the private sector. Federal laws that preside over personal data protection are usually for specific sectors, such as health and insurance (Health Insurance Portability and Accountability Act - HIPAA), banking (Gramm-Leach-Bliley Act - GLB), telecommunications (Telecommunications Act) and consumer issues (Children’s Online Privacy Protection Act - COPPA). The majority of states have a specific legislation for personal data protection, but California stands out in the privacy settings for having issued the first and most dynamic laws on the subject. The novelty in US regulation framework is the recently approved Cloud Act, which determines American tribunals’ competence to demand access to data stored in other countries.

Considering this diffuse regulatory scenario, the United States does not have a specific organ that concentrates all aspects of privacy and personal data protection. Authority over these issues at the federal level is exercised by independent bodies responsible for ruling and assuring the compliance to sector-based standards. One example is the Department of Health and Human Services – HHS, which rules over and assures compliance to data protection in the health sector. Another is the Consumer Financial Protection Bureau that has adopted parameters to defend these rights in the financial sector, under the contents of Gramm-Leach Bliley Act.

Outside the industrial context, the Federal Trade Commission - FTC<sup>lxvii</sup> takes on the lead role in privacy regulation and enforcement. Section 5 of the Federal Trade Commission Act is the main tool used by the institution to assure citizen privacy, having a general clause on consumer protection, and prohibiting unfair or deceptive acts or practices in the consumer environment.<sup>lxviii</sup> Although it does not give the institution the power to charge fines, it allows the Commission to apply measures against the violation of its rules, and these measures have often generated administrative ordinances that forbid companies to repeat negligent conduct and possible biannual audits for up to 20 years.

Moreover, the FTC has investigative prerogatives regarding compliance to its rules.<sup>lxix</sup> In general, the Commission files a complaint when it has reason to believe that a specific individual is using (i) an unfair method of competition or (ii) an unfair or deceptive act or practice. After the complaint is filed, an administrative law judge (ALJ) receives and analyzes the litigation, and the parties may appeal the decision to the entire composition of the Commission. This process may result in a cease-and-desist order, which the FTC can enforce through an injunction or a civil penalty request in federal courts.<sup>lxx</sup>

Within state matters, attorneys general also have the responsibility of applying enforcement measures for commercial practices considered unfair or deceptive, and handling violations defined by state privacy protection laws.

In addition to this institutional overview, we may say that there are considerable self-regulation practices in the United States. Given the concerns regarding privacy and the absence of a specific state regulation, private entities have, for example, adopted privacy policies, and have started to use seals/certifications and other mechanisms capable of certifying that a determined company follows the adopted policies.<sup>lxxxvi</sup> This exists alongside a fragmented co-regulation regime, developed by sector agencies through the establishment of private enforcement measures. In other words, there are penalties arising from the non-compliance of Codes of Conduct, Ethics Codes and clauses formulated by the companies themselves and ratified before the regulating organ.<sup>lxxxvii</sup>

### c) Uruguay

Uruguay is emerging as a leader in Latin America regarding personal data protection. It was the second country to be recognized by the European Union for promoting the adequate protection of personal data and the first non-European country to ratify Convention 108 of the European Council.<sup>lxxxviii</sup>

In Uruguay, the protection of personal data is constitutionally defined as a human right (Article 72) defined by Law no. 18.331/2008 (Ley de Protección de Datos Personales y Acción de Habeas Data - LPDP).<sup>lxxxix</sup> This convention assures data subjects the right to control how their data is used, when data is either physically or digitally stored. It also assures the possibility to present a habeas data to public and private entities to exercise such right.<sup>lxxx</sup>

The competent organ to assure the respect to this right is the Unidad Reguladora y de Control de Datos Personales - URCDP, established by LPDP as a technically autonomous body linked to their National Agency for the Development of e-Government - AGESIC.<sup>lxxxxi</sup> URCDP is linked to the budget of the AGESIC and is responsible for the standardization, inspection, cooperation, sanctioning and management of international data transfers. URCDP also issues opinions (dictámenes)<sup>lxxxii</sup>, develops good practice guides (guías de ayuda)<sup>lxxxiii</sup>, assists the Executive Power and issues statements requested by other entities. As for penalties, the LPDP endows the URCDP with the power to apply administrative sanctions such as the observations, warnings, fines, suspension and closing of databases, promoted with the support of the Judiciary Power.

The URDCP is led by an Executive Council formed by three members, one being the Executive Director of AGESIC and the two others named by the Executive Power, required to have a personal and professional history of knowledge on the matter. These specificities seek to ensure the members of the authority have independence, efficiency, directness and fairness in the development of their functions (Art. 31 of LPDP). With the exception of the Executive Director of AGESIC, the other members have a four-year mandate that may be renewed. The directors keep their post until the end of the mandate, except when removed from their post by the Executive Power for incapability, omission or crime, following due process of law.

The LPDP, as a support structure of the Executive Council, established a multi-sector Advisory Council, formed by five members, (representatives from the Judiciary, the Public

Prosecutor, the academy and the private sector) who have a recognized background in advocacy and promotion of human rights. The Advisory Council may be asked by the Executive Council to analyze matters within its responsibility and is required to consult on cases of regulatory exercise by the Executive Council.

Those responsible for databases covered by the law are required to register at URCDP.<sup>lxxxiv</sup> Based on this registration, URCDP fulfills its mandate to disclose freely to any individual the existence of personal databases, their purposes and the identities of those responsible. LPDP also states that no database can have purposes that violate human rights or are contrary to the law or to public morale.

Additionally, the URCDP can also register Codes of Conduct developed by associations and representative bodies for privately owned databases, provided that the URCDP determines them to be legally compliant.

#### 4.1.2. Regulatory Possibilities for a Brazilian Authority on Personal Data Protection

This section proposes options for institutional design of a Brazilian Authority on Personal Data Protection, indicating possible regulation models and their related financial tools, composition and responsibilities will be presented.

The goal is to briefly cover the latest advances in the debate and to explore the presented alternatives, focusing on the appropriate type of model and its subsequent composition, financing and management arrangement.

Considering all the relevant information, the most appropriate regulatory model to govern and oversee Internet privacy is the establishment of a central co-regulatory authority and incentives for interim self-regulation practices. There should be encouragement of private sector initiatives for suggestion of Codes of Conduct and sector standards for Internet personal data protection, given the lack of a competent co-regulation authority.

Regarding the current debate on a competent authority, the public consultations conducted by Congress on personal data protection showed certain common general characteristics<sup>lxxxv</sup> that must guide the creation of the authority.<sup>lxxxvi</sup> For the most part,<sup>lxxxvii</sup> the conclusion is that there must be a unique, centralized authority, subject to the participation of relevant actors, formed by an expert technical team, of independent finances and decision-making.<sup>lxxxviii</sup> However, some opinions do not support establishment of a new authority, considering that the country already has a series of bodies with legislative competence or to regulate and apply the current legislation.<sup>lxxxix</sup>

The concerns raised in the public consultations can viably be addressed by regulation and co-regulation models,<sup>xc</sup> provided that the established body has the authority to make decisions, has financial autonomy and is subject and responsive to sector demands. This would affect coexistence of self-regulatory initiatives, given that they do comply with current legislation and regulations issued by the competent authority.<sup>xcii</sup>

In any event, self-regulation is insufficient to duly regulate and enforce privacy on the Internet, especially in mid and long-term. That is because self-regulation experiences are often not

multi-sector (or “multi-stakeholder”), but depend on the voluntary adhesion of different actors. Also, standards issued through self-regulation are not mandatory and the body will have limited sanctioning capacity.

Despite this, purely regulatory models are not appropriate, considering their complete and excessive sector impermeability that may result in a slowdown not just in development of Internet applications, but also personal data protection models and other related matters. Currently, the Brazilian governmental bodies are not capable of adequately handling the matter, at times lacking know-how, organizational capacity or necessary resources to regulate and inspect personal data protection.

Given the current context of spending cutbacks in Brazil, there is less chance for expansion of already existing governmental capacities or instituting a new organ within the structure of direct or indirect public administration, as could happen with technical and organizational capacity of SENACON or establishment of a specific Regulatory Agency for personal data protection.<sup>xcii</sup>

Within this scenario, the co-regulation model represents a viable alternative to handling matters related to Internet personal data. That is because it reduces the State’s financial and organizational onus, with shared responsibilities. It is a tool capable of combining the flexibility of self-regulation with the mandatory characteristic of governmental norms. In other words, co-regulation enables a structure linked to democratic channels that informs the competent authority, while also dealing with complex technical debates and the needs of a growing market of intense technology use, mainly transnational, with substantial asymmetry of information, therefore being seen with much more acceptance from the private sector.<sup>xciii</sup>

In this regard, some interesting examples of co-regulation already exist in Brazil, such as the Electric Energy Chamber of Commerce (known as “CCEE”) regarding sector regulation. The Chamber is a non-profit inspected by ANEEL, with the goal of promoting electric energy trade among the sector.<sup>xciv</sup> Formed by consumers and agents affiliated with electric energy services and installations, it is supported by contributions from its agents and donations. Therefore, CCEE is a private organization, maintained by private resources, established with legislative authorization and regulated and inspected by ANEEL. Beyond this, it can mediate transactions in a regulated sector and present proposals to change issue electric energy commercialization procedures to the Agency.

Similar to this is NIC.br, also a private association with the capacity to regulate the system of Internet domain names and numbers in Brazil. It is self-financing, with resources from the registration of “.br” domains. Although it does not act as a normative body, it has advisory capacity in different fora, having been legally recognized within the Internet Framework for its contribution to matters involving exceptions to the principle of network neutrality.

These examples show the viability of establishing a co-regulatory model of a Personal Data Protection Authority. Other institutional examples that may serve as a model will be outlined below. The recommendation, therefore, is to create a central and independent authority, protected from the politics or specific sector pressures.

An example is the case of the European Data Protection Authority, previously explored in detail, which consists of a central body to guarantee privacy in all Member States, with the capacity

to advise institutions of the European Union and of national authorities, and overseeing standards compliance and conducting investigations.

The authority must have a technical staff – not only for technological matters, but also for legislative, economic and market issues. Technical staff is essential in this sphere, due to the sophistication and rapid change in related issues and diffuse regulation by distinct authorities, which results in inappropriate regulatory and inspection environment with high transaction costs. Beyond this, the authority would also need to deal swiftly with complex and immediate issues, such as information leaks, crises or cybernetic attacks.

The response to such scenarios currently depends exclusively on institutions such as the Legislative or Judiciary Branch, both lacking the required speed or technical capability to deal often immediate and complex issues.

Beyond the specific expertise to handle the particular privacy protection issues in IoT applications, the authority must collaborate with multiple sectors, involving representatives from government, business and industrial sectors, the scientific community, civil society and the academy, among others. Creation of standards involving different actors gives the project legitimacy and stimulates voluntary and independent compliance due to the possibility of sanctioning. Similar to this is the URCDP Advisory Board and its Working Group established by Article 29 of Directive no. 95/46/CE of the European Parliament, with a multi-sector composition and to support Uruguay's and the EU's data protection policies.

Concerning the authority's competencies, they range from the ability to issue mandatory standards and inspection and enforcement activities. The normative proposals previously debated in National Congress provided for the possibility of the authority issuing standards complementary to federal legislation, auditing the handling of personal data, promoting education on data protection, adopting measures for security incidents, managing international data transfers and imposing various penalties (such as warnings, fines and the suspension of activities).

The range of competencies suggested in the Bills was considered appropriate, especially the promotion of social awareness, inspections, imposing of sanctions, issuing of opinions and standards related to personal data protection and publishing of public databases.<sup>xv</sup> The URCDP in Uruguay has similar competencies, working with standardization, inspection and sanctioning. There is also required registration of companies that collect, handle and transfer personal data. In addition, the possibility of this authority sanctioning and inspecting for compliance with standards or codes of conduct developed in a self-regulation regime is considered beneficial, as in binding corporate rules in the European Union.

An additional area would be acting as an ombudsman, with mechanisms to receive and investigate individual complaints on poor management of personal data by companies and public authorities. The European Commission's Data Protection Officer is somewhat analogous, as the role involves cooperation with authorities of the Member Countries of the European Union, dialoguing with collected data subjects and maintaining a registry of operations involving personal data conducted by the Commission.

The personal data protection authority must have unique and identical competencies to manage data collection, use, handling and other operations both in the private and public sector. A robust protection of privacy is the basis for the development of applications of smart cities, open government, as well as any other governmental services that use data. The public sector therefore will also need to observe and be subject to guidelines adopted by the personal data protection authority. An exception is described under the scope of smart city privacy within this book. The Federal Constitution makes no distinction whatsoever between the right to privacy and private life in the private and public sectors; the recommendation, from an institutional point of view, is that law and the authority to deal with the issue of isonomy, without distinction based on the sector to be analyzed.

Finally, regarding financing, the simplest solution would be a specific budget endowment. This assures organizational regularity and is present in the current models of both the European Union and the United States. There are, however, other possibilities. Some examples are solutions mentioned in the public consultation, such as the model implemented in Spain, in which the Agencia Española de Protección de Datos (AEPD) is maintained by the fines it imposes.<sup>xcvi</sup> Nevertheless, the model may encourage issuing of fines to collect resources, without observing coherent decision-making for imposing penalties for infractions in personal data collection, handling and sharing.<sup>xcvii</sup>

Another solution for financing the Brazilian authority would be an adaption of the Uruguayan model, requiring the mandatory registry of databases. The fee for registry could be used to finance the institution. However, there are some obstacles related to this financing model, among which are the need for an explicit legal provision and the charging of additional amounts, as well as the imposition of costs for additional transaction costs for the sector, which could discourage registration.<sup>xcviii</sup> Among the possibilities, there is also financing through contributions from interested sectors. In this case, a criticism would be the possibility of financing agents having undue influence on the body.

In any case, independent of the model adopted, the systemic benefit of a unified personal data protection authority would far outweigh any incidental cost. The current situation is one of increasing transaction and regulatory costs. The uncertainty resulting from the current personal data protection legislation and its consequent costs are greater than financing any kind of protection authority model.



## 5 Information Security

IoT is characterized by the mass adoption of low-cost devices and sensors, which often do not meet minimum security standards, connected to networks that are at times unsecured. Added to the "open borders" nature of incidents and the possibility for vulnerability expansion is concern for network and device security.

The timing is opportune. Data shows that Brazil ranked second in financial losses from cybercrimes in 2017 (around US \$22 billion), outranked only by China.<sup>xcix</sup> During this period, approximately 62 million Brazilians experienced incidents such as hacking and distributed denial of service attacks (in which data traffic resulting from a multitude of devices is directed to a server to overload it).<sup>c</sup>

In order to deal with this scenario, governance models are being discussed both for international cooperation and in relation to the Brazilian internal institutional arrangement. At the local level, in order to encourage the adoption of protective measures for information security by private initiative, alternative must be found, either via adoption of voluntary mechanisms for device certification or by observation of minimum-security criteria in critical infrastructures.

One area that could lead to concrete measures is voluntary security certification of devices connected to the Internet of Things. The structuring of a certification system based on voluntary self-assessment, without legal obligation, can potentially create a culture of transparency in the provision of information to the user and in encouraging the adoption of a high-security standards by private initiative. An option could be creation of an "alliance" with representatives from the private-sector, which could be responsible for structuring and developing guidelines.

### 5.1 Governance and International Cooperation

The possibility of adopting a new model of international governance in cybersecurity is currently under discussion, given the "open borders" aspect of information security incidents and the expansion of network vulnerabilities with the development of the Internet of Things.

One option mentioned is the possibility for the International Telecommunication Union (ITU) to lead the discussion, possibly through a World Summit on Cybersecurity. This would be based on the model established by the World Summit on the Information Society, adopted in 2003 in the ITU.<sup>ci</sup> The objective would be creating an environment dedicated specifically to information security among countries, with an organized structure to foster international cooperation.

However, it is understood that the ITU is not the appropriate venue for eventual measures, as it is not a multi-sectoral forum.<sup>cii</sup> Decision-making within the organization primarily involves Member States and private initiative, without the participation of a plurality of representatives and sectors of society in the discussion, which is considered essential for creating successful information security policies. Brazil defended this position within the Inter-American Telecommunication Commission ("CITEL"), part of the Organization of American States ("OAS"). In CITEL's contribution to the ITU-led World Telecommunication Conference in 2012 ("CWG-WCIT12"),

Brazil affirmed that aspects of national security and cybercrime were not addressed by regulations within the scope of the ITU.<sup>ciii</sup>

Notwithstanding the criticisms of ITU participation in this area, the discussion on international cooperation among countries to fight cybercrime is essential in the context of the Internet of Things, for assuring a secure environment for the development and operation of solutions and applications. To this end, improvement of current mechanisms for the prevention and treatment of incidents between countries is essential, and will be addressed below.<sup>civ</sup>

The current international reference tool for police cooperation in cyber-security is the Budapest Convention on Cybercrime ("Convention on Cybercrime"), adopted in 2001 by the European Council and ratified to date by 52 countries, mainly by Member States of the European Union.<sup>cv</sup> The instrument establishes the minimum standards of protection in order to allow the collection of data and data storage by foreign authorities. Although the text does not define how each Member State should legislate, it defines the specific attributes that should be included in the scope of domestic legislation.

However, the general consensus is that the Budapest Convention is in many respects outdated in terms of technological change. Moreover, the instrument did not enjoy widespread international adoption, being ratified by just 52 countries.

Brazil did not adopt the Convention on Cybercrime.<sup>cvi</sup> One reason is because Brazil only adheres to international treaties in which it has participated in negotiations. Another reason is the many criticisms of the text of the Convention due to the lack of progress resulting from technological developments since its adoption in 2001, as mentioned, and imbalance between measures for police cooperation and respect for fundamental rights of the individual.<sup>cvii</sup>

While the Convention allowed for greater consistency among legal systems of the Member States, by means of the established minimum protection criteria, that standardization comes too late. This is because some of the main Member States, notably European countries, are revising their internal rules on cybersecurity and even entirely repealing data retention regimes related to the Convention, especially in the wake of the decision of the European Court of Justice that considered national laws on data retention "unconstitutional" as it pertained to European regulations.

Given the situation and the alternatives set forth, we believe that any move towards joining the Convention on Cybercrime would have a negative effect. This is because such adherence creates the possibility of conflict with the Brazilian legal system, which cites, in a preliminary form, the requirement of respect for the fundamental rights of the individual by the Federal Constitution, such as the right to freedom of expression and privacy.<sup>cviii</sup>

A better way to address the issue of cybersecurity in IoT at the international level would be to seek other forms of international cooperation, taking into account the efforts being made by countries such as the United States, Canada, Japan, China and Korea.

As an alternative to joining the Convention on Cybercrime for international cooperation, countries may engage bilaterally in Agreements on Mutual Protection and Exchange of Classified

Information, a strategy adopted by Brazil. Such a strategy would produce more significant effects than would adherence to a Convention that already appears to be outdated and awaiting updates. Brazil already has a series of current bilateral agreements with countries such as China, Canada, Cuba, Mexico, France, Nigeria, Panama, Suriname, Colombia, Peru, Portugal, Spain, Russia, United Kingdom, Sweden.<sup>cxix</sup> Seeking new agreements would enrich the national legal system, while ensuring that it would remain *pari passu* with the most current cybersecurity standards.

Such agreements allow active and passive direct assistance among countries and the exchange of institutional experiences and best practices, for example. To illustrate, it is possible to request an active assistance order in a criminal investigation or case, so that the courts of a determined country may assess the merits of the request for cooperation, in accordance with its domestic law. On the other hand, passive assistance works in reverse, with a foreign authority sending a demand for cooperation to Brazilian authorities.

Compared with adherence to the Convention on Cybercrime, Agreements on the Mutual Protection and Protection of Classified Information offers benefits, such as the flexibility resulting from creation of specific partnerships with countries where there is interest, sophistication and greatest possible updates of the legal order. It is necessary to emphasize, however, that the system fails in corresponding the cross-border flow of data. In certain cases, there is no certainty as to what information can be obtained by authorities, with who and under which specific conditions.<sup>cx</sup> In the context of the development of IoT solutions, this problem can be exacerbated. One of the foreseen challenges would be the identification of the application provider responsible for an IoT solution and principally, the location of its database, due to the supposed increase in complexity in the data flow between the various actors involved in providing a solution.<sup>cxii</sup> However, we understand that constant revision of the base text of these agreements will have a positive effect on the entire legal order, resulting in updating of previous agreements when necessary.

Another way is to facilitate international police cooperation, with respect to the guarantees of fundamental rights established by the national legal system, creating new instruments for doing so and reviewing other instruments currently in force. For example, the adoption of international instruments that promote incentives for the exchange of strategic information and the exchange of human resources between agencies to protect the information security of countries should be prioritized, as suggested in the base document of the Brazilian Strategy for Digital Transformation, developed by the Inter-ministerial Working Group created by Ordinance No. 842 of February 17, 2017.<sup>cxiii</sup>

To complement this, we also suggest increasing Brazilian activity within the OAS, to strengthen regional and international cooperation in cybersecurity. Interfacing with the OAS has been historically relevant for development Brazil's policy on information security and cybersecurity. Brazil has already enacted the Inter-American Convention on Mutual Assistance in Criminal Matters through Legislative Decree no. 272/2007.<sup>cxiiii</sup> Within the organization, the Inter-American Committee Against Terrorism ("CICTE") develops the Cyber Security Program, focusing on security and critical infrastructure. CICTE has been relevant in developing the topic in the OAS Member Countries, including Brazil.

Also important is the country's effective follow-up in defining international standards, as well as self-regulation or hybrid regulation regarding cyber-security issues. Encouraging or even requiring suppliers of IoT equipment, software, and other inputs to be certified by international organizations (such as the IEEE, among others) is an effective, low-cost institutional pathway that can produce immediate results. In this sense, promotion and monitoring of standards-setting processes and other coordination measures are recommended.

Another issue that needs to be considered, in terms of reciprocal assistance and even for fostering international development, is cybersecurity. For economic reasons, developing countries such as Brazil utilize a large volume of inexpensive connected devices that do not meet minimum safety standards nor can be maintained and updated in terms of security. The set of devices are then transformed into liabilities, in the form of negative externalities, as well demonstrated by denial of service attacks through botnets such as Mirai or Persirai. In this sense, it is in the interest of the international community and the OECD countries to develop mechanisms to foster development, in the form of credit lines, loans and other funding, which can assist developing countries in dealing with these issues. With this, connected devices would not pose a risk to critical infrastructures located in other countries. Our conclusion is that today cybersecurity must be one of the components in promoting international development. Investing now could result in great savings in the future, for developing countries as well as for OECD members.

## 5.2 Brazilian Institutional Arrangement

For development of effective cybersecurity - and especially for the Internet of Things – promotion of institutions whose common goal is multisectorialism is essential. That is, cooperation is needed from different sectors such as the public power, private sector, academia, technical and scientific community and civil society, among others. No cybersecurity policy can be effective if only conducted by one of these sectors (or mainly by one of them). For cybersecurity to be effective, rapid response mechanisms that simultaneously involve cooperation among all these various sectors is essential.

Although in Brazil there exist information security standards, there is no defined governance among these actors, nor an institution that promotes multisectorialism in this area. Given this, we suggest an information security strategy within the scope of the Federal Public Administration, with creation or designation of a body or entity capable of coordinating activities based on information security. This body should have the effective role of "coordinator", functioning as a forum (or hub) for joint multi-sectoral action. There is a number of feasible alternatives for the designation or creation of this body, as will be demonstrated in the pages that follow.

From the outset, it must be emphasized that an institutional governance model on information security in Brazil could be effective if there is as base of this necessary interaction between the State, private initiative, academia and civil society. This is a recommendation found in specialized literature,<sup>cxiv</sup> including governmental and public policy discussion,<sup>cxv</sup> through contributions from the private sector<sup>cxvi</sup> and from other governments.<sup>cxvii</sup> In other words, there is evidence showing that a multisectoral approach works to promote effectiveness of any institution that deals with the topic of cybersecurity.

It is worth noting that, according to a rule of exclusive responsibility in the Federal Constitution, the initiative to create a specific organ in the Federal Public Administration to deal with the subject of information security must originate from the presidency of the Republic.<sup>cxviii</sup>

Among the possible institutional models would be the creation of a permanent multisectoral information security council, with the participation of the public power, private initiative, scientific community, civil society and academia. From a material point of view, the council could act in an advisory capacity in the development of national cybersecurity policies and can also serve as connection hub, providing, for example, the creation of mechanisms to respond to information security incidents (rapid response), whenever necessary, with the ability to unite various sectors of society for maximum effectiveness.

This council should provide an appropriate structure for the protection of information security, within the IoT development environment, and for the coordination of cooperation between the organs and government entities. As an example, there is the possibility of such a structure being linked to a specific Ministry, such as the Ministry of Justice, which would enable this Ministry to act in a technical and transversal manner within the scope of the Federal Public Administration. In addition, within the scope of the Ministry of Justice, the council would be integrated with the Federal Police, allowing even greater ability to respond to security incidents that affect the country's critical infrastructure, as well as to combine cybersecurity issues such as the fight against cybercrimes. This structure would not be entirely new within the Ministry of Justice, as it already directs multisectoral committees, such as the National Council for Combating Piracy, among others, in addition to direct interfacing with the Institutional Security Cabinet (known as the "GSI/PR").

Positive aspects of this model include openness to collaborative participation among Federal Public Administration bodies, the private sector, civil society and academia. The model can create a positive impact by creating an environment of trust between the Public Power and the private, public and academic realms. This trust is essential for cybersecurity issues. Another positive point arising from the proximity to civil sectors is the complementary action of the Institutional Security Cabinet, which, in turn, focuses on protection of information within the exclusive scope of the Federal Public Administration. This option is also recommended as does not imply further expansion of the public machine.

In the future, if feasible, we believe that another possibility to manage information security in the long term would be the creation of an independent regulatory agency specializing in cyber security. The agency should be competent to deal with risk management, incident prevention, education programs and international cooperation, and to develop good practice guidelines focusing on private initiative, certification of devices and definition of minimum safety criteria. The same element of multisectoral cooperation must also be present in this agency. With this, there is the possibility of establishing cooperation with representatives from academia, civil society and industry, so that the agency's actions are not excessively influenced by the State, or the private sector, and avoiding undue interference in the agency by its own regulators or other special interest groups.

### 5.3 Encouraging Adoption of Security Certification Criteria for Various IoT Components

One of the main problems in adoption of IoT devices on the user side (be it an individual or business-to-business) is the lack of information on security measures and other functional characteristics of connected devices. In general, there is little transparency regarding privacy and security risks of using such a device, and the practices and duties of the solution provider.<sup>cxix</sup> If provided with accessible information about, for example, encryption and access management, the end-consumer can make more conscious choices about the device purchased. For example, awareness-raising measures could help the consumer avoid an IoT solution that may, for example, cause a short circuit, leak personal data, or allow connected home devices to be controlled by an unauthorized third party.<sup>cxx</sup>

On the developer side, a model for certification could encourage companies to increase their security standards, provide information with transparency, and invest in building a culture of confidence and trust.

To make this possible, we suggest the adoption of a voluntary certification system, with the adoption of signaling seals and systems ("voluntary certification"). The objective is to create a mechanism to demonstrate the provision of information and suppliers' and manufacturers' commitments to good practices.

We must note that we are not proposing the replacement of required compulsory assessment for products, services and processes, such as those under the scope of INMETRO or ANATEL. On the contrary, we suggest the adoption of a tool that is a complement to the mandatory compliance assessment by the State, focusing on privacy and security by design.

In both cases, what is needed is certification of products that can be connected to the Internet of Things, with penalties in the event of non-compliance. Under the scope of INMETRO, these products may be "toys", "equipment for water consumption" and "safety of household and similar appliances".<sup>cxxi</sup> In the ANATEL plan, a certification and homologation of products for telecommunications would be required.<sup>cxxii</sup>

We believe that the adoption of a voluntary certification model could also lead to increased sharing of information about vulnerabilities, with the involvement of academia and the information security research community.<sup>cxxiii</sup> While sharing information about known risks and attacks benefits the market as a whole, the greatest challenge remains public sharing of relevant information and the lack of existing incentives to do so. This bottleneck is amplified by the absence of a predefined model for information sharing.<sup>cxxiv</sup> Another challenge is the lack of clarity provided to private initiative about the benefits of sharing information on vulnerabilities. By fostering the creation of a trusted environment, the device certification model can, as a consequence, encourage the sharing of vulnerability information by IoT device developers.

As a means of implementing the certification, signaling and indication, the suggestion is to create an "alliance", comprised of relevant private initiative representatives engaged in the development of IoT devices, in a model of self-regulation, based on multisectoral consensus.<sup>cxxv</sup> We initially consider this to be the most advantageous model. Firstly, because private initiative operates many of in IoT solutions and has expertise, and any certification initiative should be organized

around the industry. Secondly, the model allows the actors themselves, rather than the State, to bear the costs.<sup>cxxvi</sup>

One possibility is the adoption of a model with ten large actors and twenty smaller organizations, involving members from the private sector and academics.<sup>cxxvii</sup> For example, an IoT Chamber can be created, a forum linked to the Ministry of Science, Technology, Innovation and Communication, which can serve as a focal point for structuring the creation of this "alliance".

The "alliance" would certify laboratories to conduct conformity assessments of product certification. Also, it could create a dedicated website for the certification of IoT devices, and produce publications on the topic of relevant information, vulnerabilities and coordinated responses.

As an example, it is worth mentioning Commercial Product Assurance (CPA), a British authority responsible for certification of information security, which makes books and guidelines available through its website to anyone interested in acting as a certification body, in addition to the general public. The publications outline certification procedures, and can serve as guidelines for laboratory operation and governance, in addition to providing the population with more detail on the information contained in certification seals.<sup>cxxviii</sup>

Here we must note that there is no single model of certification, signaling and indication, but a myriad of possibilities. Among the possible alternatives, suggestions include the "voluntary" model, without legal obligations to adopters. In this, the provided information is the initiative of the developer, and not a legal obligation.

It is important that the private sector sees certification not as a cost, but as a means to add value to products, with long-term engagement. This relates to consumer awareness, with information consumers may choose to purchase more secure certified equipment, which could be seen as a competitive differential for the market. In this sense, the certification model is paralleled by relevant awareness-raising initiatives, in particular information sharing on security incidents from the Brazilian Computer Emergency Response Team ("CERT.br"), an agency that acts as a focal point for private initiative in case of incidents and attacks.<sup>cxxix</sup>

A self-assessment model for device certification is recommended. According to this model, the device provider submits the relevant equipment information to the body responsible for certification. To ensure credibility, they should submit a self-assessment to the entities accredited by the "alliance", who are responsible for verifying the information and granting the certification seal.<sup>cxxx</sup>

However, the certification model should not impede entry of smaller actors nor reflect the interests of specific actors. The self-regulation should offer flexibility by not locking in certain technologies. Therefore, the focus should be on certification of non-proprietary technologies or creation of technologically neutral certification profiles, that is, ones that do not consider specific technology, but only minimum-security criteria.

This arrangement should be low cost, allowing small actors and products to participate in the system. In certain jurisdictions, certification of IoT devices can reach 500,000 euros, as with smart

electric meters in the European Union, through the Common Criteria (CC) method of credentialing.<sup>cxxxix</sup> In this context, the voluntary model of self-assessment provides greater agility and lower cost in obtaining certification.

We would like to point out that adoption of self-regulation (“bottom-up”) information security strategies rather than State regulation is not unprecedented. On the contrary, it is a common initiative in other jurisdictions. As the DigitalEurope organization points out, the model is a trend in countries such as the United Kingdom, the United States, Japan and Italy.<sup>cxxxix</sup>

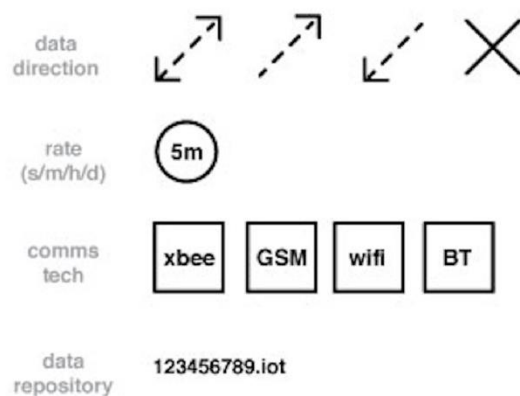
In the European Union, of note is the Trusted-IoT certification, discussed as an alternative to the models regulated by the economic block.<sup>cxxxix</sup> In another model, the Online Trust Alliance, linked to the Internet Society, is dedicated not just to fostering certification of IoT devices, but also to public policy efforts for information security.<sup>cxxxix</sup> Open and innovative, the #iotmark certification offers transparency in the development of its certification criteria.<sup>cxxxix</sup>

Transparency must be the basis for certification, not just during the creation of certification profiles under the scope of the "alliance", but in providing product information to the end consumer. The following should be highlighted: (i) device security, with information about security measures adopted and data on functions and processing; (ii) credentials and possibilities for user access; (iii) connectivity; (iv) remote updating of security measures.

The objective is to level the playing field for the application developer and the end-consumer, who may be uninformed regarding the product’s technical characteristics. To address this, we suggest that information be available to the consumer through clear and easy-to-understand visual resources, such as a label or seal on the product or packaging. This would be based on the model of the Brazilian Labeling Program, coordinated by INMETRO, which provides energy efficiency information labels to consumers.<sup>cxxxix</sup>

Below we present some concrete examples, according to the Mozilla Foundation:<sup>cxxxix</sup>

Product seal model developed by the Designswarm agency provides basic-level information on IoT device data traffic.



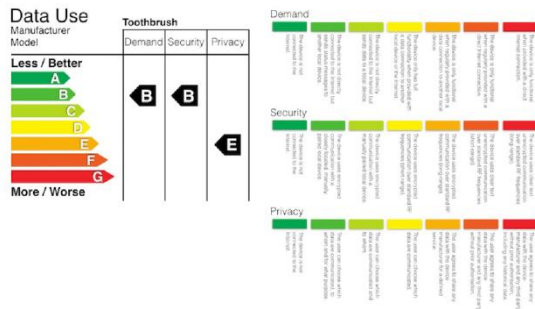


This template for product seal developed by the agency Beyond.io, provides basic information on the sharing of personal data collected by IoT solution.



Model for product seal developed by Boris Adryan, which provides technical information on data consumption, security and privacy.


Demand	Security	Privacy
The device is only functional when provided with a direct internet connection.	The device uses clear text unencrypted communication over standard RF frequencies (long-range).	The user agrees to share any data with the device manufacturer and any third party without prior authorization, including any historical data.
The device is only functional when regularly provided with a direct internet connection.	The device uses clear text unencrypted communication over standard RF frequencies (short-range).	The user agrees to share any data with the device manufacturer and any third party without prior authorization.
The device is only functional when regularly provided with a data connection to another local device.	The device uses encrypted communication over standard RF frequencies (long-range).	The user agrees to share any data with the device manufacturer for a defined service.
The device only has full functionality when provided with a data connection to another local device or the internet.	The device uses encrypted communication over standard RF frequencies (short-range).	The user can choose which data are communicated.
The device is not directly connected to the internet but sends data to a local device.	The device uses encrypted communication with a manually paired local device.	The user can choose which data are communicated and to whom.
The device is not directly connected to the internet but sends status messages to another local device.	The device uses encrypted communication with a closely located, manually paired local device.	The user can choose which data are communicated, to whom and for what purpose.
The device is not connected to the internet.	The device is not connected to the internet.	The device is not connected to the internet.



Model for product seal developed by Thorne & Bihr, which provides basic information through icons about collection, storage and sharing of personal data by devices.



Model of the seal adopted by the "Digital Standard" initiative, which aims to create an industry standard for information about the device's software and hardware characteristics, describing indicators and operating procedures.<sup>cxxxviii</sup>

Test Name	Criteria	Indicators	Procedure Overview
<b>Security (Is it safe?)</b>			
<b>Build Quality</b>			
<input checked="" type="checkbox"/> <b>Best Build Practices</b> 	The software was built and developed according to the industry's best practices for security.	The product was built with effectively implemented safety features.	Run static analysis software to determine what application armoring features are present.  Are there Stack Guards, and if so, are they effectively implemented?  Are all safety features available in the pertinent OS enabled? (e.g., ASLR, CFI, RELRO, DEP, etc.)  Are those safety features well implemented and/or enabled with optimal settings? (E.g., High Entropy ASLR, rather than just Dynamic Base on Windows 10)  Are the binaries 32 or 64 bit?

In due course, with advances in the voluntary certification model, however, the self-regulation arrangement could evolve into a co-regulation or hybrid regulation. This would include the participation of a multi-sectoral council or public agency focused on information security, if one of these bodies is eventually created within the scope of the public power. In this model, the state body can entrust the certification of devices to private initiative, but could continue to determine guidelines and requirements.

The action of the council or agency would be development of guidelines for the evaluation of product compliance and issuance of certifications and for the sharing of information on infra- and intersectoral vulnerabilities.<sup>cxxxix</sup> It could also work for adoption of measures to stimulate education and awareness about information security, through the organization of workshops and the execution of research and development programs, in partnership with private initiatives, academia and civil society. The agency could also sign agreements with foreign agencies for simplification of procedures and sharing of information on risks and vulnerabilities.

#### 5.4 Information Security in Critical Infrastructure

An important aspect of information security is ensuring security of critical infrastructure, such as sanitation and electric energy networks.<sup>cxli</sup> Within the context of IoT development, there is a tendency to increase connectivity of such essential systems, which in turn increases information security requirements for these sectors, given the potential social impact caused by a possible attack or security breach.

In Brazil, a structure for critical infrastructure security already exists. Decree no. 7.009/2009 relegated this to the Chamber of Foreign Affairs and National Defense ("CREDN"), presided over by the Chief Minister of the Institutional Security Cabinet.<sup>cxlii</sup> Under the scope of the Federal Public Administration, the Information and Communications Security Department (known as the "DSIC"), also linked to the Institutional Security Cabinet, published the Guia de Referência para a Segurança de Infraestruturas Críticas de Informações ("Reference Guide for the Security of Critical Information Infrastructures") in 2010, which still serves as a reference for institutional models.<sup>cxliii</sup>

Strengthening the institutional structure dedicated to critical infrastructure security within the scope of the Federal Public Administration is suggested, maintaining the Institutional Security Cabinet in the coordination of efforts and the establishment of partnerships with technical centers specialized in the subject. There are benefits in the current structure, such as Institutional Security Cabinet issuing of security norms of the Public Administration. The immediate objective should be to further foster existing sharing of information on vulnerabilities and experiences between management bodies and entities, as well as to provide assistance in the event of security incidents and to raise awareness of servers, as suggested by the Infrastructure Guide from DSIC.

The activities of CREDN can be guided by awareness-raising activities, with interaction between the Institutional Security Cabinet and public administration bodies and entities (e.g. Ministries), technical centers (e.g. CTIR Gov), and partnerships with private initiative and academia. Once again, the interface and coordination between the various sectors permit constant communication and exchange of information between them, always managed in an institutional way, can greatly contribute to the effectiveness of this policy.

In parallel, CREDN, the Institutional Security Cabinet, and the Ministries responsible for specific critical infrastructure sectors could be entrusted with the responsibility of developing "best practices guidelines". These guidelines should serve as a reference for private initiative and address methodology for implementing security measures and certification criteria. For example, concessionaires in the energy and basic sanitation sectors, mentioned above, are much in need of a defined minimum criteria for information security.<sup>cxliii</sup>

Regarding the electric energy sector, the generation, transmission and distribution of energy is largely depending on secure information.<sup>cxliv</sup>

However, there exists minimum security requirements by ANEEL or within the National System Operator (known as the "ONS"). To mitigate vulnerabilities in the sector, the suggestion is for ANEEL to create a roadmap for prevention of security incidents, detection, response and crisis management. Additionally, it is suggested that ANEEL adopt a security that would assist concessionaires in meeting minimum aspects of information security, such as the definition of functional security architecture, risk analysis, definition of network maturity and internal training. These are minimum and basic steps to address the issue, without negatively affecting the adoption of other measures.

Regarding the sanitation sector, there are concerns about attacks that could allow access to infrastructure and potentially modify water monitoring and treatment systems, affecting the provision of this essential service. Alongside adoption of computerized systems, security protection structures should be implemented. To this end, we suggest the adoption of information security policies by service providers, such as municipal agencies.

Moreover, all critical sectors of the country should define a minimum protocol to define a roadmap and to identify the essential responsibilities, attributions and institutional interfaces within the government and with other actors of society, without negatively affecting future measures for adoption.

## 5.5 Blockchain Technology for Device Certification and Guarantee of Digital Identity

In addition to the measures already addressed in IoT information security, we believe that blockchain technology may serve as a promising resource to safeguard IoT solutions and network security.

Blockchain can be seen, roughly speaking, as a public or private ledger with flexible and broadly customizable access distribution. Each event is aggregated into the blockchain with unique identification by an encrypted hash code, creating an immutable "block" sequence. If any intrusion or fraud is detected, there will be no "consensus" on the network, so the breach of security will be identified.

The possible benefits for IoT stem from two fundamental attributes of the technology. First, the blockchain can allow the authentication of the identity and origin of a device, individual or entity connected to IoT. Second, it can verify the integrity of the data collected from the certified devices.

Digital signatures, usually in an encrypted hash code, through the use of digital certification are used for authentication of events and objects in the blockchain. In practice, this digital certification enables the permanent cataloging of information necessary to ensure network security, such as object and developer identity, list of available software updates, and known security vulnerabilities.<sup>cxlv</sup>

The mechanism provides a time stamp for data collected by authenticated devices and sensors, which makes it possible to identify the origin of any inclusion in the ledger.<sup>cxlvi</sup> With this, any modification to information after its collection can be identified, providing the network with high transparency and reducing the risk of falsification and intrusion. There are initiatives that allow for verification of the integrity of video recordings, obtained from surveillance cameras connected to a network. Each stored record is linked to a specific hash, immediately recorded in the blockchain ledger. This makes manipulation attempts futile, since the hash of the modified file will not be parallel to the hash recorded in the blockchain.<sup>cxlvii</sup>

The certification of devices to ensure network security has been studied and implemented in other jurisdictions. In 2016 in the US, the Department of Homeland Security funded a proof of concept for an IoT blockchain solution, focusing precisely on the detection of components (i.e. ability to associate devices with a particular network), authentication (i.e. ability to verify the origin of devices and prevent falsification), and control of updates (i.e. ability to control and schedule device software updates).<sup>cxlviii</sup> In another proof of concept, the US Department of Energy subsidized a solution for the use of blockchain to protect smart-grid networks, through automatic detection of invasion attempts and anomalies in collected data.<sup>cxlix</sup>

The possibility of using blockchain is gradually being analyzed in Brazil. Examples of this can be seen in Central Bank and the Brazilian Federation of Banks tests for its use in the banking sector.<sup>cl</sup> The Center for Research and Development in Telecommunications (CPqD) has also produced a white paper specifically analyzing authorship and auditing in the blockchain.<sup>cli</sup> This demonstrates the formation of a growing technical ecosystem in Brazil capable of implementing the technology.

However, there are limitations in unified digital certification according to the Public Key Infrastructure (known as ICP-Brazil) model, instituted by Provisional Measure No. 2.201, of July 27, 2001. The standard touches upon the legal validity of the declaration of authorship, authenticity and integrity of electronic documents for authentication through digital certificates issued in accordance with the ICP-Brazil standard.<sup>clii</sup> The model faces practical and structural challenges, to be outlined below.

First, digital certificates are marketed at high cost, which makes it impossible for them to be adopted by the absolute majority of the population. Currently, a digital certificate costs between R\$180 and \$460 and is valid for between one to three years. At this time, only about four million certificates have been issued thus far, despite the system's more than 16 years of existence. The data is symptomatic: only 1.3 million of these are linked to individuals, which corresponds to a minimal proportion of the Brazilian population.<sup>cliii</sup>

Second, governmental approval of the ICP-Brazil structure creates market reserve, with negative effects on innovation and positive repercussions, such as the use of blockchain for the digital certification of objects in IoT. This model goes against good international practices, which allow for greater flexibility in hiring a certification body and there is less risk of market abuse and failure. We consider the most coherent model to be one in which the market remains open, so that certification may be granted by either public entities or by private initiative.

Blockchain can be used to reverse this situation and democratize access to digital certification, which would be a significant advantage in IoT information security. The technology could create independent digital certification models that are less expensive and more reliable, auditable and transparent, and with greater security compared with ICP-Brazil certification model.<sup>cliv</sup>

For these reasons, improvement of the ICP-Brazil model implemented by Provisional Measure no. 2.200-1, of July 27, 2001 should be considered. The goal is to create models in which any interested party can certify IoT devices with legal necessity, without a link to ICP-Brazil.

At a moment when billions of devices are expected to connect to the IoT, with varying degrees of compliance with security measures, new technologies such as blockchain may allow manufacturers to certify and validate their devices, authenticating objects, individuals and entities within IoT. The result would more evolved security and protection against attacks and falsifications in networks connected to the IoT.

## 6 Net Neutrality

The Public Consultation on the Internet of Things indicated concern regarding the role of net neutrality in development of the IoT ecosystem in Brazil. In Brazil, the Internet Framework has established a general rule of net neutrality, determining the obligation of isonomic treatment of data packets for the intermediaries that operationalize the data transmission in the network.<sup>clv</sup> The standards are for data traffic at the network infrastructure level.

Objectively speaking, the Internet Framework net neutrality rule prohibits technical discrimination of data traffic in terms of content, source, destination, terminal or application. While the Internet Framework generally places the onus on the "person responsible for transmission, switching or routing," the Final Report of the Senate Special Committee determines such obligation for "connection providers, telecommunication companies, backbones, switching services, packet routing and other agents working in the operation of the Internet."<sup>clvi</sup>

Despite the implementation of the net neutrality rule, the Internet Framework allows two exceptions, outlined in an exhaustive list. First, it prioritizes traffic for emergency services. It then prioritizes data packets in terms of technical requirements required for the provision and proper usage of services and applications.

In terms of exceptions, there are three necessary conditions: not causing unjustified harm to the user, respect for free competition and for transparency. In addition, the net neutrality rule was regulated by Decree No. 8.771/2016. Decree no. 8.771/2016 is mainly dedicated to determining criteria for exceptions to the duty of isonomic treatment of traffic; it establishes the conditions under which arrangements are allowed between the party responsible for transmission, switching and data routing and application providers, such as zero-rating and sponsored access.

Regarding the exceptions to isonomic treatment, Decree No. 8.771/2016 makes clear that this is an exceptional measure, permissible only in two cases as listed in the Internet Framework: indispensable technical requirements for the adequate provision of services and applications and prioritization of emergency services.

In both cases, conditions listed by the Internet Framework must be met cumulatively. For indispensable technical requirements in the adequate provision of services, Decree no. 8.771/2016 clearly establishes that only the treatment of network security issues or network management in exceptional congestion situations can be considered as such in this case.

It should be noted that the approach allows for network management by data traffic controllers, provided that the goal of the practice is preserving the stability, security and functionality of the network, within the limits established by ANATEL and the Brazilian Internet Steering Committee (CGI.br.).

In terms of emergency services, the regulatory decree is equally clear when stipulating a full list of hypotheses for discrimination or traffic degradation. These are the risk of disaster, emergency or state of public calamity, as well as communication between communication providers of emergency services.

Regarding the commercial agreements between the party responsible for the traffic and the application provider, Decree No. 8.771/2016 effectively seeks to extend the protection of net neutrality to plans known as zero-rating, in which connection providers exempt the resulting traffic of certain content of the user data franchise, and sponsored access, in which the application provider pays the cost of data traffic by the user.

However, it should be noted that Decree No. 8.771/2016 does not surpass the limits of the law by banning zero-rating plans or sponsored access, insofar as there is no discrimination in data traffic. Therefore, if the offering respects the isonomy in data packet traffic, then the standard would not be violated.

Additionally, it is important to note that Decree no. 8.771/2016, in Article 2, sole paragraph, exempts the application of the net neutrality rule for networks for (i) telecommunications services that are not directed at providing connection to the public Internet,<sup>clvii</sup> and (ii) specialized services, provided that they do not constitute a substitute for the Internet and are intended for specific groups of users.

This exception is important as many IoT support and application networks fall into categories designated as exempt by Decree 8.771/2016.<sup>clviii</sup> In this way, concerns about so-called mission-critical IoT applications (such as some IoT applications for the healthcare environment) can now be addressed based on the current regulatory standards, without any need for modification.

In summary, given the concerns indicated by the Public Hearing regarding the importance of net neutrality for the development of the Internet of Things, it should be stated that Brazil has modern and adequate regulation for development Internet innovations, guaranteeing the protection of isonomic treatment on the Internet, so that it is not necessary to change the net neutrality rule, provided for in the Brazilian Civil Rights Framework for the Internet, to promote the development of the Internet of Things in Brazil.



## II – ANALYSIS OF PRIORITIZED ENVIRONMENTS

### 7 Smart Cities

#### 7.1. Introduction

##### a) Concept of “Smart Cities”

Currently, more than 50% of the world’s population lives in cities and projections show that by 2050 this number will rise to 60%, with an increase of 2.5 billion people living in urban areas.<sup>clix</sup> Considering these high rates of urbanization, the introduction to IoT solutions will mainly support strategies for greater efficiency of services in urban centers.

The concept of smart cities is associated with the use of new information and communication technologies to optimize the planning and management of public policies in the urban environment. Although it is considered a crucial topic in global discussions on economic and social development, there is no consensus on its concept, since the idea of a smart city is relatively new and constantly transformed. This is because urban experiences with smart services evolve differently based on the specific policies, goals and even financing models in each city.<sup>clx</sup>

The narrowest definitions of smart cities focus on the installation of information technology systems along with other city infrastructures and public services, connecting them and enabling them to collect and analyze different types of data. On the other hand, broader definitions define smart cities as those in which investments in technological structures serve sustainable economic growth.<sup>clxi</sup> Even the employment of word smart is questioned when referring to the relationship between the city and technology. Some say the use of such a vocabulary may lead to technocratic discourse, promoting the virtualization of interpersonal relations in the urban environment and ignoring the inherent limitations of technologies.<sup>clxii</sup>

However, there is no doubt that information and communication technologies (ICT) play an important role in the process of modernizing urban systems, as they can potentially improve relations among government, the private sector and citizens. An example would be real-time information on municipal public transportation fleets or different fees for electricity through the installation of smart meters in residential units. Thus, the purpose of the technological improvements described throughout this chapter relate to improving services to those living in urban areas.

Although ICT represents an essential component, smart cities are more than just a simple technological apparatus of public structures, since innovation efforts by Public Power must consider citizens as the starting point.<sup>clxiii</sup> Therefore, among the various regulatory descriptions described in this work, we point out concerns regarding users of municipal public services, such as the approximation between citizens and the Public administration through greater governmental transparency;<sup>clxiv</sup> and issues of safety and privacy of information generated and stored by IoT devices.

In this scenario of many possible definitions of smart cities, there is a number of areas that could be improved by the use of IoT technology. To exemplify, there are projects with objectives such as:

- Improving institutional governance to make public data available and to educate citizens, to increase access and analysis of available data, as well as mechanisms for popular participation in public management;
- Sustainability and cooperation in environmental protection through automated waste collection and clean energy production;
- Implementing electric smart grids, capable of reducing energy waste, improving allocation of investment in the grid, reducing consumer fees, among others;
- Automating water and sanitation supply network which, similar to the case of smart grids, improves the measurement system and reduces commercial and non-commercial losses; and
- Improving citizen experience with traffic and public transportation, through collection and instant analysis of traffic, bicycle and pedestrian flow data, for example.

b) Data Collection as a Key Point of “Smart Cities”

As shown by the examples presented, the promotion of a smart city is closely related to the implementation of new technologies by the Public Power. This is because IoT in cities, with the ability to improve the quality of life and experiences of citizens, oftentimes must be executed in tandem with or exclusively by a governmental body. Moreover, certain smart cities environment are regulated sectors. As such, the respective Agency must study and modernize sector norms to enable the implementation of new technologies in public services and to promote security when adopting innovative policies.

This characteristic of smart cities is of particular concern, since public service provision is increasingly tied to collection, storing and sharing of personal data. As widely shown in this book, the collection and use of data collected through IoT technologies promotes countless benefits for cities in the provision of public services. Such data may be collected within the framework of federal regulation and local policies, but data collected and made available by federal bodies is also of great value.<sup>clxv-clxvi</sup>

Therefore, it is essential to adopt measures capable of preventing the illegal use of data and surveillance of people by the State or by private agents. The first step was the approval of specific legislation on personal data protection. However, law’s efficiency may be undermined due to the lack of a personal data protection authority, with competence to issue regulations and opinions to guide public administrators and private agents.

There are also concerns related to storage of data by public bodies, due to information security and regulation of cloud computing services. In the current scenario, federal regulations regulate contracting of IT services by the Federal Public Administration, establishing minimum qualifications for contractors,<sup>clxvii</sup> information security guidelines<sup>clxviii</sup> and the need for data

communication services<sup>clxix</sup> to be provided by federal public administration entities.<sup>clxx</sup> There are also regulations from the Ministry of Planning (MPDG) and the Institutional Security Cabinet<sup>clxxi</sup> on hiring cloud services, which establish hiring parameters and information security guidelines. The Ministry of Planning in particular establishes the need for Public Federal Administration data and information to be stored exclusively in national territory.<sup>clxxii</sup>

In spite of Federal Public Administration having a more detailed legislation, it shall observe LGPD's provisions just the same as individuals, public agencies or other federal powers or spheres. Considering that, so far, there were no legislation and that public policies of smart cities were mainly developed by the cities themselves, the rules for Federal Public Administration contracts were to be used by local bodies as a model for contracting of cloud services in IoT applications. After LGPD's approval, public policies and Federal Public Administration rules are to be compliant with federal law.

#### c) Drones and Smart Cities

Another perspective in city environment involves the use of drones<sup>clxxiii</sup> for solutions in IoT and other applications.<sup>clxxiv</sup> The commercialization and use of these aircraft in Brazil has specific rules defined by ANATEL<sup>clxxv</sup>, ANAC<sup>clxxvi</sup> and DECEA.<sup>clxxvii</sup> According to relevant regulations, the safe use of drones with a maximum takeoff weight of over 250 grams in the urban area requires, among others: (a) an operation at least 30 horizontal meters from buildings, installations<sup>clxxviii</sup> and people not involved in the operation;<sup>clxxix-clxxx</sup> (b) buying insurance with coverage of damages to third parties;<sup>clxxxi</sup> (c) not using autonomous drones;<sup>clxxxii</sup> (d) that each drone pilot operates only one equipment at a time; and (e) the compliance to the requirements established by DECEA for the use of airspace.<sup>clxxxiii</sup> The Public Power is exclusively exempt from the above-mentioned insurance and respecting of the minimum distance from third parties, as long as it meets the applicable regulatory requirements.

Drone operations must comply with all other requirements and obligations applicable to each case, as determined by the indicated regulations.<sup>clxxxiv-clxxxv</sup>

#### d) Chapter Scope

The vast possibilities of this subject made it necessary to restrict the object of study of smart cities to the following cases, to be covered in greater detail:

- Smart public lighting: Use of sensors to monitor burnt-out lights and to optimize the use and substitution of public lighting assets;
- Smart power meters: Reduction of costs related to reading meters and theft prevention;
- Control of traffic and public transportation: Use of data obtained by cameras, cellphones and sensors to monitor traffic and optimize traffic, pedestrian and bicycle flows; and
- Crime monitoring through video/sensors: Use of closed-circuit TV and an audio-monitoring system to enable real-time response and coordination, as well as predictive analytics from historical data.

Considering that IoT development in smart cities involves contracting and implementation of specific devices by the public administration, possible forms of ICT contracts will also be briefly addressed.

Considering the limited nature of this, the study of smart cities' regulation will present the latest in technology and the legislative challenges related to privacy in the cities and for each of the selected applications (e.g. smart public lighting, mobility and public safety), as well as a debate on ICT contracting by the public power.<sup>clxxxvi</sup>

## 7.2. Privacy in Smart Cities

The increasing use of technological devices dispersed throughout urban space, capable of collecting data on citizens, monitoring their activities and even identifying them, raises a number of questions concerning the protection of individual privacy and personal data.<sup>clxxxvii</sup> To make the public planning of smart cities a successful reality, it is imperative to prioritize a guarantee of citizen privacy in the act of implementation. Therefore, in addition to the Public Power adopting good management practices that consider the previous diffuse legislation on the subject (in particular the Internet Framework and Decree no. 8.771/2016) and recent legislation with uncertain application (LGPD), we consider the efficiency of specific personal data protection legislation very important to preserve fundamental rights.<sup>clxxxviii</sup>

Given the various possibilities for use of personal data in smart cities, we describe below the main challenges in privacy protection and then follow this with an outline of possible alternatives to minimize these challenges.

### a. Personal Data Collection

As a first step in the analysis of legal obligations to protect data within IoT solutions in smart cities, it is necessary to identify the expectations of citizens in terms of privacy in public environments such as streets, parks, squares and other open areas in private environments.<sup>clxxxix</sup>

In relation to private environments, the doctrine assumes full application of legal protection in an uncontested form,<sup>cxk</sup> with the expectation of full control over personal data in private locations. However, the situation is more nuanced when it comes to public places.<sup>cxci</sup> Part of the doctrine considers it unreasonable for citizens to expect privacy in public places<sup>cxcii</sup> while, on the other hand, a more conservative group advocates full respect of privacy in public environments as well. As citizens must be able to determine which information will be disclosed to third parties, there is therefore valid expectation of privacy and respect of private life, even in public places.

From this premise, the implementation of projects connected to the Internet of Things in public environments in smart cities involves both scenarios, one of "personal" data collection that enables the identification of the data subject, and another in which, hypothetically, information collected through devices and sensors does not enable citizen identification. This is a classic case in the civil doctrine related to the right of image. Photographs of "the crowd" in which it is impossible to identify any individual are allowed. However, photographs that individualize someone who walks

on the streets are not permissible, except when there is conflict with another well-defined public interest (as in criminal investigations or procedures, for example).

For solutions that do not collect personal data – such as a photograph of “the crowd”, in which data is anonymized and aggregated – and conducted by either Public Power or by the private initiative, there is no requirement to comply with the data protection legal regime or to obtain prior authorization to collect, process, store and share data.

Such an example might be sensors that collect information and monitor pedestrians’ behavior and flow through heat maps to analyze urban mobility, as individuals are not identified, and only calorimetric information is recorded. Other examples not involving personal data collection relate to gathering technical data such as air humidity, pollution rates, noise levels, temperature, atmospheric pressure, and radiation, among others.

However, other IoT solutions situations in smart cities do imply personal data collection. In these cases, a list of norms and practices is applied in both public and private sectors.

When private initiative implements IoT devices, it is subject to full legal obligations from the Internet Framework, Decree no. 8.771/16 and other sector standards. Valid consent to collect, handle, use and transfer personal data is required. It must also furnish information on the purpose of handling, storing and sharing the data. The alternative is to collect data in an anonymized and aggregated manner, which would disqualify it as personal. However, there must be objective certainty that the data cannot be deanonymized, enabling individuals to be identified through technical means or by crossing data with other databases and thus, re-establishing the data as personal data.

As for the governmental use of IoT devices in smart cities, the body or public entity collecting data must respect the legal framework and personal data protection, except when the collection is necessary for essential public services to be provided, for public good.<sup>cxciii</sup>

Clearly, there will be many cases in which the identification of individuals will be required in order to provide essential public services. Given the importance of these services, citizens do not have the possibility to “opt out” of services with a built-in IoT solution. In a large city like São Paulo, for example, residents cannot simply “choose” not to use the public transportation service, as they depend on it for their daily commutes, and consequently, their economic survival. In such cases, even if the user “consents” to the personal data collection within the use of the service, the consent is not free, expressed and informed, considering that the user depends on that service. Therefore, there is an additional responsibility from the Public Power in these cases, since personal data will inevitably need to be collected, regardless of the will of the user or the public service. As already mentioned, data can be collected, but the Public Power must ensure its security, and comply with the specific end to which data was collected, being prohibited from transferring data to third parties unrelated to the provision of the service.

The exemption from the obligation of obtaining the data subject’s consent to collect data and enable public service provision mirrors the models implemented by jurisdictions considered advanced in citizen privacy, such as the European Union and, within Latin America, Argentina and Uruguay. The Uruguayan case is interesting since it is a developing country in the same regional

context as Brazil. Uruguay allows personal data to be handled by the Public Administration without previous consent when data processing is necessary for the provision of “State duties”<sup>cxciiv</sup> such as essential public services, as previously exemplified. As for the European Union, the EU 2016/679 General Data Protection Regulation, of May 2018, establishes that public bodies and entities can handle collected personal data without consent in necessary cases, according to the public good or in the exercise of the public authority.<sup>cxciv</sup>

One specific issue is the use of IoT solutions for monitoring through surveillance cameras, in which citizen identification is aligned with the purpose of guaranteeing public security, as in monitoring centers implemented in Rio de Janeiro and São Paulo.<sup>cxci-v-cxcvii</sup> In such cases, data collection without prior and express consent is justified, as long as it is used strictly for the purpose for which it is intended (public security), is necessary, proportional and handled exclusively by authorities of that public security system. <sup>cxci-viii</sup>

Based on previous considerations, it is clear that the Federal government, States and Municipalities are responsible for ensuring the privacy of citizens as a priority in the implementation of any type of smart city. It is necessary to adopt specific legislation, capable of covering all federative spheres and ensuring citizens’ privacy (through a series of guarantees, including the principle of legitimate interest, purpose, transparency, right to rectification, the principle of necessity and proportionality, among others), and authorizing data collection by the Public Administration as long as it is limited to specific purposes related to the provision of the service in question. It is worth remembering that, in terms of the Constitution, privacy is defined on the same level as other fundamental rights.

In addition to the described scenario, the Public Power can also collect, through IoT solutions in smart cities, personal data not linked to the provision of public services. In such cases, legal authorization is required, as well as compliance to the usual legal framework for personal data protection. Valid consent is also required for public bodies and entities to collect data, as well as legal authorization that determines the limits and purposes for it.

Another issue is the Public Administration receiving data collected by third parties, such as private entities. In these cases, there must be special attention to evaluation of compliance in receiving such data, as well as the chain of custody and the authorizations inherent to their use, including by the Public Administration.

This is the case of the augmented reality solution implemented in the city of Santander, Spain, by the Smart Santander project to boost tourism and entertainment.<sup>cxci-x</sup> The solution involves the provision of information on tourist spots and interactive and customized experiences to citizens through a mobile application. Data collected by sensors distributed around the city, as well as the use of QR Codes, and the crossing of databases between the city and the private initiative indicated users’ points of interest, while the collection of geolocation data and the identification of user browsing habits enabled case-by-case customization, according to each citizen profile. Such uses are welcome but imply the need of caution from the Public Administrator, who should verify if the company handling the data has the necessary authorization to collect them, obtained through free, express and informed consent and if this consent also covered the transfer or use of data specifically by the Public Power and to what purposes.

Another relevant issue in smart cities is the qualification of the data collected or obtained, be it by solutions provided by the Public Power or by private initiative. Although the Internet Framework and its regulatory Decree do not distinguish between the types of personal data, all three Bills on personal data protection are currently before Congress – Bills no. 5,276, 2016, 330, 2013 and 4,060, 2012 – distinguish “personal data” from “sensitive personal data”. “Sensitive personal data” would usually refer to personal data on racial or ethnic origin, religious and political beliefs, as well as data on health and sex life. If one of the above-mentioned Bills is approved, this distinction is of great relevance, since the collection of “sensitive personal data” must comply with more strict criteria for obtained consent, such as the provision of prior specific information of the individual and an individual expression regarding collection of sensitive data.<sup>cc</sup>

Therefore, if sensitive personal data is collected by IoT solutions in smart cities, there is a more complex scenario for the collection of valid consent, with an increased risk of violating the legal framework in privacy and data protection. One example is the increasingly widespread technology of facial recognition. A recent study by Stanford University showed that it is possible to infer data such as sexual orientation (data considered sensitive by all major global privacy laws) just by analyzing an individual’s face.<sup>cci</sup> This illustrates the problems involved in the collection and use of “sensitive personal data”, which should involve extensive caution, curbs and counterbalances. Once again, it is essential to have legislation that guarantees the constitutional rights of citizens of privacy and is a preliminary and necessary step for implementation of technologies that collect “sensitive personal data”, such as facial recognition.<sup>ccii</sup>

Considering the problems described in reference to personal data collection in the urban environment, it is advisable that, first, personal data collection by the Public Power through IoT solutions occurs in an anonymized and aggregated way, through robust cryptography criteria and the usage of practices such as differential privacy, among others.<sup>cciii</sup> The goal is to inhibit information collected without consent to identify a specific user, in order to avoid State violation of the constitutional principles of protection to privacy and private life, as provided in infra-constitutional norms such as the Internet Framework (Article 7, IX c/c Articles 10 and 11).

In other words, data collection must be planned within the concept of privacy by design, meaning that the design of a public service must consider the dimension of privacy protection from its conception. Thus, a solution would be for data to be anonymous and aggregated from the moment of their collection. Other techniques, such as the use of “differential privacy”, must also be employed as ways to assure even more robust techniques to protect the private life of individuals.

As observed, apart from the collection inherent and necessary data for the provision of essential public services, public bodies and entities that wish to collect data for purposes beyond the needs of the service must implement mechanisms to obtain valid consent through the provision of clear and specific information.

In this hypothesis, a first possibility would be to publicly disclose a Privacy Policy for every IoT solution through an opt-in tool on a website or through a mobile app, in which the user would agree to the terms and conditions for data collection. Other than the opt-in, offering an opt-out tool is essential, so that individuals may stop, at any time, the collection or handling of their own personal data. However, none of these solutions expresses the need for these matters to be broadly and generally regulated by the law. The city’s own privacy policy may be defined by municipal law when restrictive to a matter of “local interest”, as in the institutional design of Public Administration bodies related to individual data protection.<sup>cciv</sup> This would provide necessary protection to citizens while also giving the city the “go ahead” to implement IoT smart services that collect personal data. In conclusion, privacy protection and authorization to implement smart services based on data are “two sides of the same coin”.

The Privacy Policy must be accessible to the public and capable of clearly informing citizens about the practices of collection, anonymization, handling, storing and sharing of data.<sup>ccv</sup> It must specifically contain information on: (i) the Administration body responsible for handling the collected data; (ii) which information is collected; (iii) the purposes for which information is collected; (iv) an overview of the recipients of shared information; (v) how to refuse collection or require the exclusion of data purposed for handling, processing and other activities; (vi) how to contact the public entity responsible for handling the data.

Another possibility is to provide information on personal data collection through visual identification at the sensor site, along with contact information. However, the low degree of formalization of IoT solutions – usually there being no law, infra-legal norm or formal instrument for public contracts – creates challenges in promotion of data protection practices.<sup>ccvi</sup>

The recommendation is that the Public Power entirely avoid collecting personal data considered as “sensitive”. If a specific general law on personal data protection is approved, the collection – or inference – of this data would represent exacerbated risk to the cities, considering the difficulties in obtaining previous consent in smart cities.

#### b. Personal Data Processing

In the area of personal data processing, one emergent problem is the use of data for purposes other than those consented by the individual.<sup>ccvii</sup> Although personal data collection may enable the Public Power to obtain information on water and power consumption, to make public security more efficient or even to leverage the transparency of governmental activities and approximation between individuals and the State, every use must specifically attend to the purpose of that service. If data is used for different purposes (or different from those supplied to the citizen in the original consent), new consent must be obtained from the citizen. If it is not obtained, then anonymization, aggregation and use of techniques of differential privacy are necessary, always in a technically secure and entirely anonymous manner.

Therefore, to mitigate the risks of using collected data for purposes other than those informed, we suggest the implementation of technical mechanisms based on the principle of privacy by design, with the design of the IoT solution implementing privacy protection mechanisms from its inception, including the use of differential privacy and anonymization techniques that may protect the privacy of users without precluding the possibility of using the database for the provision of public services.<sup>ccviii</sup>

Other than that, data processing raises the issue of vigilance surveillance of the individual by public authorities and bodies, with no express legal provisions available. The engagement and debate about the possible uses of data collected by the Public Power are essential not only to foster governmental transparency but also to avoid the so-called “panoptic effect”, under which the uncontrolled monitoring surpasses the benefits of obtaining data for the provision of public services.<sup>ccix</sup>

While the Public Administration provides vast options for IoT solutions in different segments, such as public security, management of water resources, and electric power supply, another emerging concern relates to the possibility of the Public Power losing control over the flow of data from these technologies. The adequate management of data collected by each IoT solution is



necessary for the Administration to have full control of the purposes to which personal data are collected.

All data used by the Public Power must comply with legislation and be of the public interest. In other words, the purposes for which the government uses its citizens' data must have legal precedent and constitute a lawful purpose.

#### c. Personal Data Storage

Storage creates recurrent concern regarding the security of collected data and technological devices used in IoT solutions, as the both feature vulnerable hardware and software.

Adoption of privacy measures by design to store data obtained by IoT solutions in smart cities, as well as for processing and even sharing data, is recommended to mitigate risks. Among possible tools are above-mentioned differential privacy, aggregation and anonymization of collected data by IoT devices.<sup>ccx</sup>

The differential privacy technique allows the data controller to anonymize statistics and consult from the original database without any modification.

Anonymization is the most rigid form of personal data protection. Through a cryptographic "key", data is anonymized and, consequently, may no longer feature this "personal data" classification, therefore being processed, stored and shared with no risk of identifying their subjects. Therefore, the immediate objective is to assure stored data does not enable the identification of citizens and permanently obscure information that enables it. Moreover, the use of cryptography to code data would prevent malicious agents from accessing information collected through IoT solutions, to protect the identity of data subjects.

There are also other measures that could mitigate risks related to personal data storage, such as "aggregated" or "grouped" data. This technique allows for data to be stored "in combination with" other data that fit under the same criteria.<sup>ccxi</sup>

#### d. Personal Data Sharing

Another important aspect of the debate on privacy in smart cities is the sharing of data collected by solutions developed by the Public Power and other Public Administration bodies and police authorities.

We must immediately note that the very act of sharing databases by the Public Power raises questions. Can an individual's mobility data be used for purposes of public security and shared with the police? Is a court order necessary? Or can citizens' data related to mobility be used by municipal tax authorities to inspect tax collection on property and services? Would a court order be necessary? Our understanding is affirmative.

The Public Power can only cross collected data beyond the original purpose to use as enforcement if authorized by the Courts. This is the consequence of constitutional protection to privacy. Otherwise, the individual would be under permanent surveillance, with disregard for presumption of innocence, good faith, with a unbalanced relationship between the State and the

public freedom of citizens. In other words, cities would become “panoptic”, in the sense of the famous prison conceived by Jeremy Bentham, in which prisoners are subject to permanent surveillance of all of their acts, even the most private. The public disclosure of protection practices used by the Public Administration to protect data could solve the challenge and prevent this problem locally.

Also, the Public Power must be prohibited from offering data collected by the Public Administration to private entities, except if there is free, express and informed consent by citizens (without any detriment to essential public services, as mentioned). An alternative could be anonymization of data in a definite and safe way, as well as aggregation of data, subject to techniques such as differential privacy, while general principles regarding purpose of data use is still respected. The mechanism does not prevent the Public Administration from using databases from IoT solutions in smart cities as a resource, but it requires any commercial usage to be limited to anonymized data, as in the development of statistics and standards.

Any partner must adopt high standards of data protection, prohibiting any sharing with other third parties, as well as any attempt at identification. Third parties, even if working with anonymized data, must commit to protection through high levels of security and may not share it with other third parties or try to employ any process with the purpose of identifying data subjects.

Moreover, the Public Administration can adopt measures through the definition of criteria for public contracting of IoT solutions.<sup>ccxii</sup> The guarantee of a partner’s compliance with legal requirements on personal data, minimum levels of managerial protection and adoption of security techniques for data protection is recommended.

The Public Power may also require its partner to employ measures such as disclosing a Policy Privacy to its users. This is the case of the “Wi-Fi Livre SP” program that, even if not related to the Internet of Things, is identified by the GEPI-FGV study “A New World of Data” (“Um Novo Mundo de Dados”).<sup>ccxiii</sup> The wording in Appendix I in the contract’s Term of Reference does prevent a partner from assigning or sharing identifiable personal data in an individualized way.

IoT-collected data could allow for cooperation between police authorities through the sharing of data between different spheres. While there exist apparent benefits and opportunities stemming from information collection for police investigations, the possibility of unrestricted access to information by police is a great concern.<sup>ccxiv</sup> When sharing data with other public bodies or investigative authorities, a previous court order within the terms of the Internet Civil Rights Framework should be obtained, which formalizes constitutional protection. Other than that, there must be limits, curbs and counterweights, respect of the principle of purposes and high protection levels by the data-receiving authority after the required court order. A possible efficient measure could be to implement management and technical training programs for public servants and police authorities on the obligations related to data protection.<sup>ccxv</sup>

In conclusion, the Internet Framework establishes the need for a previous court order to furnish users’ personal data from Internet solutions, except in cases provided by the Law. Administrative authorities can only access personal information without a court order when expressly provided for by the Law, such as in the investigation of crimes of money laundering or

concealment of properties and values (article 17-B of Law no. 9.613/1998, “Money Laundering Law”) criminal conspiracy (article 14, paragraph 3 of Law no. 12.850/2013) or in the terms of the Access to Information Law – Law no. 12.527/2011), always complying with the definitions in this legislation and the principles of need and proportionality.

e. Access to Data Collected by Controllers

Bodies and entities are subject to the duty of information promotion, provided by article 37 of the Federal Constitution, and must observe the transparency regime provided for by the Access to Information Law. The Law requires that public bodies provide citizens with information of public interest, independent of request (active transparency) or upon demand from the citizen (passive transparency).

The Law considers as information of public interest what is “produced or held by an individual or private entity consequence of any bond with bodies or entities, even if this bond is terminated”. However, “personal” information concerning an identified or identifiable individual is excluded. These are of restricted access and require consent to be provided.

As a result, data that identifies or enables the identification of citizens, collected by public bodies and entities through IoT solutions in smart cities, may not be accessed or publicly disclosed, unless there is consent by the data subject and when the consent is valid (as previously mentioned, the consent may not be valid if in the sphere of or required for the provision of an essential public service).

Notwithstanding the scenario provided by the Access to Information Law, we recommend that the Public Power provides anonymized information on data collected by IoT solution to the population. This provision of information can take place through statistics reports, without the possibility of identifying data subjects. Open Data NY in New York City is an example and is a leader in use of big data for information access.<sup>ccxvi</sup> Through its website, the public can access cataloged data from more 1,400 sources, on topics like education, energy and environment, health, public transportation and public safety. The information is anonymized, without identifying individuals.

f. Mechanisms for the Exclusion and Rectification of Personal Data

According to the Internet Framework, the personal data subject has the right to solicit the removal of data provided to an Internet solution, by request, when the relationship between the parties is terminated or when the data is no longer necessary for the purposes indicated to the citizen. In absence of a specific personal data protection law, the provisions of the Internet Framework are considered as applicable mandatory legislation for the collection of data by IoT solutions.

In the scenario of the Internet Framework for IoT solutions in smart cities, there is a range of questions to consider, such as the possibility of verifying a period of data storage by the Public Power and how individuals can request the exclusion of data.

This is because there may not be tools with the IoT solutions capable of identifying which personal data should be excluded or even capable of allowing that removal. Additionally, a potential

scenario might be one in which personal data is collected by sensors in smart cities and shared with other bodies of the Public Administration, but without adequate control over access.

Therefore, Public Power should determine which data should be excluded after a certain time period, also preserving the tool that enables data exclusion in an automated way. This is the case of the LinkNYC program, in which images collected by surveillance cameras are removed after seven days, except for images kept for the investigation of incidents.<sup>ccxvii</sup>

To assure legal certainty and minimize room for interpretation, approval is needed for a specific law for personal data protection in Brazil that addresses the issue of personal data exclusion by the Public Power and defines obligations of Public Administration bodies and organs in the exclusion of personal data. Moreover, we find it fundamental to define and publish strategies on the subject of privacy in other local plans, such as for states and cities.

### 7.3. Smart Electric Power Grid

The operating logic of the power sector is traditionally based on centralized generation and unidirectional flow of energy through transmission lines and distribution networks. However, with the adoption of new technologies, some of which include machine-to-machine communication, this service model has undergone significant changes and allows the formation of so-called smart electric networks or smart grids.<sup>ccxviii</sup>

Smart grids are different from the classic electric power distribution model in that they include information from technology, measurement and monitoring devices.<sup>ccxix</sup> The addition of these new technologies in the power grid assures, among other things, the expansion of the network through multi-directional services, faster and more numerous data transmissions, the use of mechanisms of smart measurement and the integration of the electric power system with other public services.<sup>ccxx</sup>

Therefore smart grids include, among other arrangements, energy transmission structures controlled by sensors capable of detecting fluctuations or disturbances, managed storage of energy not consumed by batteries, and processors capable of controlling and responding to demand.<sup>ccxxi</sup> Such a system requires the implementation of an infrastructure capable of processing and analyzing great volumes of information, which would allow for better management of energy resources, increasing operational efficiency of the grid through the reduction of losses and transmission failures and through the decrease of consumption by the concessionaire.<sup>ccxxii\_ccxxiii</sup>

Due the importance of Smart Grids, various governmental bodies have been studying and issuing regulations since 2010.<sup>ccxxiv</sup> ANEEL in particular has held many public consultations on resolutions related to smart grid technology topics, such as a small distributed generation or the possibility of implementing variable fee systems. The National Congress has also debated bills related to the subject, such as Senate Bill no. 84/2012 and Congressional Bills no. 3.337/2012, no. 3.138/2015 and no. 2.932/2015.<sup>ccxxv</sup> In general, the bills determine replacement of electromechanical meters, the implementation of integrated communication systems between

meters and a grid management center, the establishment of minimum standards for the meters and a possibility of establishing variable fees.

Despite this scenario and the fact that the electric energy sector may benefit from broad machine-to-machine technology implementation, the analysis of the smart grids regulatory environment will be limited to the application selected by the consortium, consisting of smart meters<sup>ccxxvi</sup>

This application relates to the control and response stage to the demand on electric power and allows, through the use of analytics, dynamic pricing based on energy availability and demand, the monitoring of transmission quality and the identification of anomalies.<sup>ccxxvii</sup>

#### a) Opportunities Created by Smart Meters

The implementation of electric meters with IoT technology directly influences means of measuring and supplying electric power, since the meters allow access to energy consumption in real-time and generate data capable of substantiating variable fee policies aimed at changing consumption patterns and reducing infrastructure investment.

The benefits and functionalities of replacing electromechanical meters with smart meters with advanced metering infrastructure - AMI<sup>ccxxviii</sup>, reach both consumers and agents in the electric power supply market. From the consumer point of view, smart meters assure more transparency in billing and allow for informed consumption control. This benefit could be potentialized if associated to blockchain technology, which can store detailed information on consumption preferences and consumer generation (such as fee and flow variations and energy supply) in a secure and long-term way.<sup>ccxxix</sup>

Additionally, devices would allow for checks on quality of energy offered by utilities, and ANEEL could determine reduced charges if indicators show levels below the established quality standard. Another benefit is generation and injection of energy into the smart grid by the consumer through a bidirectional energy flow.<sup>ccxxx</sup>

On the other hand, utilities using these devices will have more control over individual and collective energy consumption, which enables the charging of variable fees by seasonal time, a mechanism called “white tariff”.<sup>ccxxxi</sup> The capacity to gather data to implement variable tariffs could encourage consumption during hours during which the grid is less overworked, with fewer hours of system overload and a related reduction of operational costs.<sup>ccxxxii</sup> Additionally, smart meters also enable utilities to offer pre-paid power, a more flexible system that adapts consumption to the consumer’s income, which could reduce payment defaults by consumers.<sup>ccxxxiii</sup>

Although smart meters can provide benefits in terms of quality and efficiency, the expense of the new devices is a challenge; they may cost 10 times more than current devices employed in the electric energy system.<sup>ccxxxiv</sup> Subsequent savings from the adoption of this technology may depend on the reasonable scalability of its production and distribution.

#### b) Competency and Regulation of Power Meters

##### Federative Competency and Decentralization

Unlike the other applications included in this study of smart cities, it is the Union's competency to legislate and manage, directly or under concession, authorization or permission, the provision of electricity services (Articles 21, XII, "b" and 22 of the Federal Constitution). There are precedents in the Federal Court that recognize as unconstitutional the state legislation that imposes power concession companies to install power meters. <sup>ccxxxv</sup>

ANEEL was established in 1996 by Law no. 9.427, and is endowed with the competency to regulate, supervise and implement policies related to the stages of electricity supply. One of its competencies is the power to decentralize some activities by partnering with Regulatory Agencies of the States and the Federal District<sup>ccxxxvi</sup>, to enable and familiarize its practices for electricity consumers.<sup>ccxxxvii</sup> Some of the states that have gone through decentralization or pursued agreements are Acre, Tocantins, Ceará, Rio Grande do Norte, Goiás, São Paulo and Rio Grande do Sul.<sup>ccxxxviii</sup>

### Regulations for Smart Meters

ANEEL, in order to regulate electricity measurement systems for consumer units, issued Resolution no. 414<sup>ccxxxix</sup> in 2010, restating the competency of electricity distributors to supply and install meters. It is also the responsibility of distributors to pay for the meters, except when expressly provided by law,<sup>ccxl</sup> such as when a consumer requests the installation of meters different from their load profile, in which case the consumer will pay for the difference in the price of the meter and for other related measuring instruments and materials. Resolution no. 414/2010 also provides that distributors have the right to choose the power meter model, provided that it complies with legal requirements and is approved by INMETRO.<sup>ccxli</sup>

The Resolution also stipulates that distributors must read power meters at intervals of no less than 27 days and no more than 33 days.<sup>ccxlii</sup> Readings using different time frames must be approved by the consumer, authorized by ANEEL or occur in specific cases as in the impossibility of accessing the meter, emergency situations or public calamity.

Given the development of new meters capable of modernizing electricity services and consumers as supplies in the energy network supply chain, ANEEL convened Public Consultation no. 43/2010 to develop a normative proposal to regulate the minimum requirements for the innovative devices.<sup>ccxliii</sup> This participatory process resulted in the issuing of ANEEL Resolution 502/2012<sup>ccxliv</sup>, which regulates the measuring system for residential, rural and other consumer categories, with the exception of low-income consumers and public lighting.

The original wording of this Resolution directed distributors to adopt the electronic measuring system within 18 months of its publication. The deadline was changed by Resolution no. 732/2016<sup>ccxlv</sup> and extended to January 1, 2018, except for distributors that established concession agreements after the Resolution was published. For these exceptions, the time limit is of 18 months from the date of the validity of their permit agreement, or from January 1, 2018, whichever date is later.<sup>ccxlvi</sup>

Therefore, starting in 2018, electricity distributors must install free meters capable of measuring active energy of four different tariff types for every consumer who asks to migrate.<sup>ccxlvii</sup> The installation must happen within 30 days of the request and consumers will be allowed go back to the conventional tariff type, which must also be reimplemented within 30 days (ANEEL Resolution

no. 733/2016). Consumers who choose not to migrate to a different tariff type are not required to install new devices.<sup>ccxlviii</sup>

Other than smart meters, consumers who choose the white tariff will have the right to see information displayed on their meter or on another device in their residence. Consumers can also request more advanced meters with functionalities such as the access to specific and individual service information. However, they may be charged for installation.<sup>ccxlix</sup>

The implementation of the Resolution raised concerns such as the approval of meters by INMETRO. However, there are reports of smart electronic meters having already been approved by the Institute, such as the equipment developed by the company Weg in partnership with electricity concessionaire AES Eletropaulo to be employed in a smart city project in Barueri/SP.<sup>ccl-ccli</sup> This shows that the INMETRO approval process is not an obstacle to the provisions of the Resolution nor an impediment to the competitiveness may reduce the price of the devices.

Since 2010, ANEEL has been facing legal challenges to implement meters that are appropriate for the new demands of the electric energy market. However, the electronic meters noted in Resolution 502/2012 are white tariff meters and do not have advanced communication systems capable of reading, selecting and collecting information instantaneously – important features for the implementation of a smart grid.

Therefore, starting June 2018, concessionaires must install, upon consumer request, smart meters specific for the white tariff. However, the demand for new functionalities and the expansion of smart grids may require a new replacement before the end of the useful life of the equipment, which shows the need for ANEEL to continue its efforts to modernize the industry.<sup>cclii</sup>

Parallel to the Agency's efforts, bills to regulate the implementation of smart devices are currently before the National Congress, suggesting some innovation to the Agency's regulations. Among them are Senate Bill no. 84/2012<sup>ccliii</sup> and Congressional Bills no. 3.337/2012<sup>ccliv</sup> and no. 2.932/2015<sup>cclv</sup> to which Bill no. 3.138/2015 was attached. Their main goals related to power meters are the extension of the meter replacement term to 10 to 15 years from the sanction of the Law, the requirement to implement a reliable communication system among all devices and the authorization and regulation of the distributed generation of energy.

Among the changes proposed by the mentioned Bills, only the requirement to implement a reliable communication system among all automation devices is considered an advanced innovation. ANEEL has been facing the main regulatory challenges to the implementation of smart meters,<sup>cclvi</sup> but advances are still necessary, especially considering that that new meters must have advanced and reliable communication mechanisms.

#### Regulation on Distributed Generation

Concerned with developing smart grids, ANEEL issued Resolution no. 482/2012 to inaugurate a micro or mini-grid electricity compensation system and to establish conditions for its supply.<sup>cclvii</sup> The resolution removed obstacles, enabling low-voltage consumers to insert energy into the electricity system, provided distributors with a means to adjust their systems to enable this

electricity generation mode and allows consumers to be compensated as they contribute to energy generation.<sup>cclviii</sup>

Despite the changes promoted by the resolution, the program did not enjoy widespread adoption, which resulted in ANEEL Resolution no. 687 in 2015.<sup>cclix\_cclx</sup> Changes herein included redefinition of micro- or mini-grid capacities, the inclusion of new distributed generation formats (such as multiple units and power-sharing), the possibility of including renewable energy resources into energy systems and the establishment of a simpler and computerized process.<sup>cclxi</sup>

In another attempt to increase adoption, the Agency in 2017 issued Circular no. 10/2017 to provide further information on the system, particularly due to the rise of new business models that were not adequately framed in previous resolutions.<sup>cclxii</sup>

According to a Technical Note issued by ANEEL in May of 2017, the regulatory changes promoted by the Agency, especially prior to Resolution no. 687/2015, resulted in an increase in the number of micro or mini-grid distributed generation consumers by year-end 2017 by a factor of 4.4. It also showed photovoltaic solar energy as the main source of distributed generation produced by residential consumers. ANEEL's perspective is that the current number of consumers will increase from 26,834 to 886,700.<sup>cclxiii</sup>

A current regulation that allows the development of distributed generation already exists. A possible challenge relates to the incidence of the ICMS tax, a competency of the states, on micro or mini-grid modes, among others. It would be important to establish, in coordination with the states, the dissemination of state laws that exempt these activities of the ICMS tax, at least while they are still incipient.<sup>cclxiv</sup>

That being said, since 2010 ANEEL has been studying and issuing regulations or technical opinions capable of stimulating the modernization of the electricity network and, more specifically, stimulating distributed generation modes. Other than that, the large number of new meters installed up to 2010 may contribute to the system for the quality of data measurements sent to the network and for being independent from the installation of an additional meter for micro or mini-grids.

#### Regulation on New Types of Tariffs

Another aspect related to the implementation of smart meters is the implementation of different consumption tariffs, among which are the white tariff and the prepayment tariff.

The white tariff was originally included in ANEEL Resolution no. 414/2010 by Resolution no. 502/2012, a voluntary tariff with different fares according to different hours of energy consumption. Its implementation conditions were later regulated by the Agency through Resolution no. 733/2016. According to current regulation, the white tariff is for residential and commercial consumers (Group B), except for low-income consumers and public lighting projects. As previously mentioned, starting in January 2018, units consuming more than 500kWh per month may choose to adhere to the white tariff, units consuming more than 250kWh per month can migrate in January 2019, and other consumers in 2020.<sup>cclxv</sup>



The white tariff will only be valid on weekdays and its fare will vary within three-hour groups (peak, intermediate and off-peak). Peak hours will be from 7p.m. to 9 p.m. with higher rates, intermediate hours with intermediate values will be from 6 p.m. to 7p.m. and from 9 p.m. to 10 p.m., and all other hours will have a reduced off-peak values.<sup>cclxvi</sup> Values charged from consumers will be detailed in their energy bills.

On the other hand, electricity prepayment is regulated by ANEEL Resolution no. 610/2014.<sup>cclxvii</sup> It is voluntary and enables consumers to cancel it at any time. Consumers who have adopted mini- or micro-grids or the white tariff will not be able to utilize this model.

Smart meters contribute to the implementation of this tariff mode, as it depends on the display of updated information on available credits to charge consumers. Electricity prepayment regulation requires meters to have a visual and a sound alarm that informs the user 15 days prior to ending of credits and power suspension.<sup>cclxviii</sup> When credits end, power may be suspended, being authorized to the distributor, at any time, the provision of a 20kWh credit. The electric power must be reactivated immediately after the consumer pays for the credit.

Although regulated by the Agency, there is divergence regarding the legality of shutting off power due to non-payment, which could create challenges to the implementation of the prepayment mode. This divergence exists because, although Law no. 9.247/1996 expressly enables turning off power for non-payment, the Consumer Defense Code provides that essential service companies must supply efficiently and continuously, prohibiting any interruptions. In any case, the modernization proposed by ANEEL appears to be viable, as the Supreme Court of Justice has been recognizing the lawfulness of power suspensions for non-payment since 2003, as long as legal requirements are observed.<sup>cclxix</sup>

It is important to keep in mind when a consumer's credits end in the pre-payment model, it may not be considered as non-payment. It only means that the consumer has not purchased additional credits. With this, the discussion does not involve cutting service, as the pre-payment mode provides for suspended service until new credits are added.

In parallel, the benefits of implementing a binomial tariff for low-voltage consumers are currently being studied. The binomial tariff consists of dividing the electricity bill into payment for consumption and for use of the power network. The implementation for this group of consumers views the compensation of concessionaires for granting access to the energy network to consumers for distributed generation. The proposal was debated in National Congress during the discussion on Provisional Measure no. 735/2016, which changed the Regulatory Framework for the Electricity Industry, but was not included in the wording of Law no. 13.360/2016. However, its implementation depends on additional studies, especially due to potential negative effects it could have on the advance of distributed generation.<sup>cclxx</sup>

In conclusion, there are also no considerable regulatory challenges related to the new tariff modes. The recent changes made to ANEEL resolutions, based on previous studies and public consultations, are aligned with the new demands for modernization of the current electricity supply system.

#### c) Personal Data Privacy and Information Security

As previously mentioned, advanced measurements provide significant benefits to the three links of three electricity supply chain: service quality assessment by the regulatory body, greater consumer control over electricity bills and reduced operational costs and investments in infrastructure for the concessionaires. However, although information and monitoring technology equipment enhances the capacity of this network to gather data, it also creates concerns regarding the privacy of electricity distribution system users and the security of the equipment.

Real-time access to electric power consumption information on individuals, residences and corporations through equipment with Internet protocol addresses (IP) and access to wireless networks, does raise concerns over privacy issues. As examples, we list: the possibility of monitoring behavioral patterns,<sup>cclxxi</sup> determining how susceptible a location is to crime,<sup>cclxxii</sup> real-time surveillance, the identification of home appliances used and the sending of undesired advertising, among others.<sup>cclxxiii</sup>

Other than that, the electricity network itself is prone to security failures. As an illustration of this type of risk, which globally affects the operational structure of the distribution system, a group of hackers has been targeting electricity companies since 2011 in both the United States and the European Union.<sup>cclxxiv</sup> According to a report issued by the company Symantec, hackers engage in cyber-espionage campaigns and, in some cases, have successfully broken into the most central areas of these companies' systems. This shows that hackers can affect the stability of power plants that supply energy on a daily basis to millions of people.<sup>cclxxv</sup>

A security failure in electricity networks (especially for equipment that monitors real-time consumption) may imply a sudden power cut in certain locations, potential alterations in the quality of the network,<sup>cclxxvi</sup> the disclosure of data on the location and consumption levels of individuals,<sup>cclxxvii</sup> and also the possibility of billing fraud.<sup>cclxxviii</sup> In fact, this is exactly what occurred in Puerto Rico in 2009, when smart meters were targeted by a massive hacking, resulting in widespread billing fraud.<sup>cclxxix</sup>

For successful planning of smart grids— primarily installation and use of smart meters —, we reiterate the recommendations previously presented in section on privacy in cities. There, we recommended that, in addition to good organizational practices by the Public Power, there should be recognition of the diffuse legislation on privacy and enactment of a specific law for personal data protection.

Given the still sparse legislation on the subject, data collected through equipment with IoT solutions (including smart meters) should involve data anonymization, cryptography and blockchain technology. This would prevent identification of any data collected without the consent of users of the electricity network.

The development of robust security models for smart systems is also recommended, to ensure, for example, end-to-end communication using cryptography and allowing communication only between pre-certified parties. Data collected by smart meters or any other IoT device in the electricity network should only be collected for the purposes of measuring consumption and managing the network.

Exceptions to this general guideline above involve valid consent from users, complying, at the very least, with the Internet Framework for cases of personal data collection (Articles 3, III c/c 7, VIII and IX). An opt-out option for users must always be available, so that users' data may not be collected for other purposes and so that they are not penalized for selecting the option.

In addition, collected data cannot be shared with third parties (unless with free, express and informed consent) or with other governmental entities (for purposes of criminal investigation, for example), except in the case of previous authorized court order authorizing such sharing.

In conclusion, the use of data for purposes other than the service provision and the management of the network must be exceptions, subject to court decision, and the free, express and informed consent of service users. It is essential for collected personal data to be protected by regulatory safeguards, which is important in the constitutional precept of privacy in this specific area.

#### 7.4. Smart Street Lighting

##### a) Opportunities Generated by the Implementation of IoT Applications

Currently, the street lighting network is undergoing important transformation due to the responsibility being transferred to cities and the possibility of using new technologies – especially the substitution of metal halide fixtures for LED (Light-Emitting Diode).<sup>cclxxx</sup> The migration to lower consumption lighting may be an important contributor in the development of IoT, as it allows the introduction of mechanisms that enable wireless communication with control and communication devices.

New fixtures will therefore be used as data network points, connected to the Internet, and are “smart” in that each point is individually controllable by software.<sup>cclxxxi</sup> This enables real communication with the control center and the bi-directional transfer of data and information.

It also enables, among other functions, the identification of real-time conditions of each fixture, the monitoring of its electricity consumption and also the use of dimmers,<sup>cclxxxii</sup> which allow the adjustment of light intensity according to the light of the environment and occupancy of the space, optimizing the use of electricity. Therefore, the implementation of IoT applications allows the smart management of the city street lighting, possibly reducing not only the city's electricity consumption but also the cost of network maintenance.

Furthermore, it is possible to integrate these services with other public utility applications, such as street security cameras, traffic lights that control street traffic and location analysis in order to generate important information for airport managers, for example. It is also possible to integrate other sensors that collect information of different types through the street lighting infrastructure. This smart city network may therefore become a source of information for Public Power in more efficient decision-making in terms of public services.<sup>cclxxxiii\_cclxxxiv</sup> However, the same precautions regarding privacy as outlined in the section on smart cities remain also apply to street lighting.

##### b) Competencies for Street Lighting Management

To begin with, when considering adjustment of street lighting to new technologies, it is essential to recall that management of street lighting services is a competency of the cities, as determined by the Constitution (Article 30, V). Therefore, even if the activity is evidently related to the provision of electricity distribution services, which is the role of the federal government (Article 21, XXI, “b”), its regulation and exploration is a municipal competency.

For this reason, ANEEL issued a resolution determining the transfer of street lighting assets to the cities (ANEEL Resolution no. 414/2010).<sup>cclxxxv</sup> This transfer of assets faced challenges, especially due to the costs of direct service provision and the physical condition of the transferred assets, which resulted in a public hearing<sup>cclxxxvi</sup> in 2013 to renegotiate the transfer period, originating in Resolution ANEEL no. 587/2013.<sup>cclxxxvii</sup>

Therefore, recognizing the role of the municipality in the provision of street lighting, cities have become responsible for activities related to the operation, maintenance, improvement and modernization of lighting networks.

### c) Street Lighting and Lighting Poles

#### Competencies for Light Pole Management and Regulation

Lighting poles are a central infrastructure for street lighting, as they support the installation of fixtures and may also be used to install IoT equipment. Light poles may be considered either as street lighting assets or as electricity assets when they are also used to support electricity wires and telecommunication services.<sup>cclxxxviii</sup> As previously mentioned, the management of street lighting is a competency of the cities (Article 30, V of the FC) and the management of electricity is a competency of the Union (Article 21, XII, b).

Therefore, the installation of IoT devices in light poles or light pole arms must comply with specific city regulation and terms of agreement that may have been established. This may imply the need to remove or observe eventual limitations for installing cameras, sensors and other IoT equipment solutions on poles. It may also be necessary to check for specific regulations on the number of units that may be installed in each light pole/arms in the city and the fees charged for infrastructure sharing.

This scenario is faced by telephone companies that wish to increase mobile Internet services by implementing antennas on street lighting poles, but are restricted by local legislation.<sup>cclxxxix</sup> For example, the city of São Paulo is currently analyzing Bill no. 751/2013,<sup>ccxc</sup> which seeks to remove obstacles for installation of a Base Radio Station in the city. Among other objectives, the Bill authorizes non-exclusive assignments of public areas and radiofrequency transmission service providers and simplifies the licensing process to install the necessary support infrastructures. Although the bill has been suspended, the city reportedly has been studying the possibility of issuing a Decree or sending a new normative text to the City Council.<sup>ccxci</sup>

On the other hand, electricity poles are property of the Union and are managed by the electricity distributor, who is legally required to maintain these public assets (Article 31, VII of Law no. 8.987/1995). For this reason, the transfer of street lighting assets provided by ANEEL Resolution

no. 414/2010 does not include the transfer of poles that support electricity distribution services, as they remain an asset of the federal public service.

Their infrastructure is shared with other services, such as telecommunications,<sup>ccxcii</sup> and therefore electricity poles also follow telecommunications regulations, such as Law no. 9.472/1997 (General Telecommunications Law – GTL) and Law no. 13.116/2015 (General Antenna Law). These regulations determine that the terms and conditions required for telecommunication companies to share infrastructure are fair and reasonable (Article 73, GTL), and that the respective Regulatory Agencies are responsible for establishing parameters for installation, operation, maintenance and removal of the support infrastructure (Article 13, I of the General Antenna Law).

#### Regulatory Scenario of Electricity Poles

Considering their shared competency of regulating the subject, ANEEL, ANATEL and ANP<sup>ccxciii</sup> issued Joint Resolution no. 01/1999, which establishes general rules for the sharing of electricity poles. The resolution provides (i) freedom to establish the price charged for telecommunication companies to install fixation points on poles; (ii) the role of the infrastructure owner in determining and managing its capacity and sharing; (iii) the obligation of approving the sharing contract before the responsible Agency.

In 2001, ANATEL issued Resolution no. 274 to regulate certain arrangements of Joint Resolution no. 01/1999, reaffirming the competency of the concessionaire to establish rules for the sharing of the exceeding capacity. The Resolution was revoked by Resolution n. 683, published in October 9, 2017, which establishes the obligation of the concessionaire to share overflow capacity of the support infrastructure when it is requested by the telecommunication service. ANEEL also issued Resolution no. 581/2002, which established minimum quality requirements for safety and environmental protection and the obligations of the concessionaires involved in the sharing of the poles.

The lack of parameters regarding contract values between concessionaires has created obstacles for negotiations, leading to the issuing of Joint Resolution no. 04/2014,<sup>ccxciv</sup> which approves the reference price of R\$ 3.19 per fixation point and establishes additional rules for the sharing of poles by electricity and telecommunication companies. The resolution also determines that a telecommunication company, individually or jointly with other companies of the same group, may only occupy one fixation point per pole, except in unusual situations and when authorized by ANEEL. However, there are no obstructions for use of the same fixation point by more than one service provider, in which case only the contracting company is responsible for paying (Article 3, single paragraph).

The Brazilian Association for Technical Regulations (ABNT) provides technical standards for sharing of poles, particularly ABNT NBR 5434/1982 – Electricity Distribution Networks in urban areas and ABNT NBR 15214/2004 – Sharing of infrastructure with telecommunication networks. These regulations present technical criteria for installing fixture points on poles, considering a space of 50 centimeters. The exact number of fixation points per pole will be determined by the concessionaire,<sup>ccxcv</sup> who must consider costs and safety and maintenance obligations for pole infrastructure.

## Considerations for Electricity Pole Regulations in IoT Services

This brief outline of the regulation is relevant for fomenting machine-to-machine policies in the country, as it involves: (i) sustainability of the system for new market players who need to use the space available on poles; and (ii) restrictions regarding number fixation points per pole may restrict the implementation of IoT devices.

In relation to the first point, the use of the reference price established by Joint Resolution no. 04/2014 for other market players may hinder expansion of installed IoT devices or the expansion of small Internet service providers.<sup>ccxcvi</sup> Alternatives may be adopted, such as the sharing of a same fixation point by more than one service or different companies who provide the same service, as in the Ran Sharing adopted by telecommunication towers in particular.<sup>ccxcvii\_ccxcviii</sup>

There is also the possibility of reducing the reference price established by Resolution no. 04/2014, which continues to be subject of lively debate among electricity and telecommunication companies. There have been previous proposals in this regard, such as the Proposed Legislative Decree no. 49/2016 presented before Congress, intended to suspend the effects of the Resolution, but terminated at the request of the author of the proposal.<sup>ccxcix</sup>

In addition, the number of fixation points per pole may represent an obstacle for the installation of new IoT devices or devices of Internet broadcast. For this purpose, it will be necessary to encourage the sharing of IoT devices by public and private services, and to invest in alternatives such as the installation of antennas on top of buildings, the implementation of underground Base Radio Stations,<sup>ccc</sup> the implementation of underground passive infrastructure, among others. However, it is important to observe the limit of fixation points per pole, as the installation of devices and wires exceeding the weight capacity of the pole may result in risks to services and citizens.

### e) Financing of Public Lighting

The financial and organizational insufficiencies of cities to expand, modernize and manage the public lighting system has led to the establishment of public lighting tariffs, which were declared unconstitutional by the Federal Supreme Court.<sup>ccci</sup> It also led to creation of autarchies or public enterprises or long-term contracts of public-private partnerships.<sup>cccii</sup> Another consequence of this paucity of municipal resources was the approval of Constitutional Amendment no. 39/2002,<sup>ccciii</sup> which included article 149-A to the Federal Constitution, authorizing cities and the Federal District to institute the “contribution to the financing of public lighting services”.

Regardless of the above-mentioned amendment to the Constitution, Municipal Laws that established contributions based on article 149-A, generally named Contributions to the Service of Public Lighting (COSIP), have had their constitutionality questioned before the Federal Supreme Court. It was the case of Extraordinary Appeal no. 573.675, in which the Attorney General of Santa Catarina questioned the institution of COSIP by the city of São José and was dismissed by the Federal Supreme Court to recognize the constitutionality of the contribution and distinguish it from taxes.<sup>ccciv</sup>

However, there is still the need for a debate on the possibility of directing funds from COSIP to the financing of PPPs that will have, among their objectives, the modernization of public lighting services, understood as an investment in the network and the implementation of IoT devices.<sup>cccv</sup> This

is of great relevance to the implementation of partnerships in public lighting, as well as for the dissemination of IoT solutions.

A particularly delicate question is the possibility of directing funds from COSIP to actions of improvement and expansion of the network, which certainly affects the possibility of having technologies added to the public lighting infrastructure, which may be integrated to the provision of different public services, such as transportation and security.

Regarding destination of funds from COSIP to improve and expand the network<sup>cccvi</sup> – which does not include the modernization through sensors and devices equipped with connectivity –, there is a process awaiting judgment by the Federal Supreme Court, in Extraordinary Appeal no. 666404 with General Repercussion recognized in November 2013. The Office of the Attorney General of the Republic filed a statement in the case, saying that the term ‘financing of the public lighting service’ is not used in restrictive or technical ways that require network improvement and expansion services to be excluded from its command, allowing the destination of resources from the contribution not only to strictly finance the lighting service, but also actions included in the process of its provision.<sup>cccvii</sup>

This debate is important as COSIP has become the main source of financing for public lighting services and it may also be possible to use it to implement new technologies with machine-to-machine support on electricity poles. The solution of this debate could support the understanding that it is also possible to use resources from COSIP to implement smart street lighting, in order to ensure more legal certainty in the publication of PPP notices on public lighting, as it could help reduce the number of suspensions by decision of local Courts of Audit caused by divergences regarding the destination of COSIP funds.

In light of this scenario and to minimize roadblocks for smart lighting projects, the possibility of presenting a new Constitutional Amendment Proposal, with the objective of adding article 149-B to the Federal Constitution, is being considered, in order to expressly authorize the destination of COSIP funds for implementation of a smart street lighting network.<sup>cccviii</sup> Another possibility would be to present it before the Federal Supreme Court, either by the Federal Government or by private parties with competency to present *amicus curiae*, explicitly expressing the issues listed above.

#### e) Financing of PPPs in public lighting

As numerous cities have no financial and organizational capacity for providing even traditional public lighting service, the establishment of Public-Private Partnerships is a very interesting option,<sup>cccix</sup> especially since the public-private partnership is a viable legal alternative, for it is a type of administrative concession (Article 2, paragraph 2 of Law no. 11.079/2004), the main option for long-term contract of public services that cannot be financed by tariffs.<sup>cccx</sup>

Unlike traditional concessions for public services (regulated by Law no. 8.987/1995), the concessionaire provides the service directly to the Administration. Here, the financing of the concessionaire would not involve tariffs, but a considered a service paid by the public administration.<sup>cccxi</sup> Therefore, clarity regarding COSIP funds is essential – as its revenue is a valuable resource for these partnerships.

Here, we should mention the possibility of PPP lighting projects relying on funds other than those from COSIP, as a possible restrictive interpretation of the use of COSIP funds does not financially impede the implementation of a smart public lighting network.

In effect, the shortage of public resources results in difficulties for Brazilian cities in implementing public service project expansion, maintenance and modernization. However, the legislation already provides the possibility of concession contracts through alternative, accessory funds<sup>cccxi</sup> and the implementation of varied funds. Beyond this, funds may be provided to PPP contracts for public lighting by charging for sharing of infrastructures to perform other public services with IoT technologies. As previously mentioned, the installation of sensors, cameras and other devices directed to the provision of public services, such as public security and mobility, may be deployed as remunerated activities.<sup>ccciii-ccciv</sup>

Therefore, understanding COSIP may provide legal certainty for PPP calls and contracts, as it will limit questioning before the Courts of Audit or the Judiciary. Despite this, although COSIP is a relevant source of funds, a possibly restrictive scenario does not impede the implementation of smart public lighting as the current legislation provides alternative financing sources that support similar enterprises.

#### f) Experiences and Capacities of Public Lighting PPPs

Contracts with private entities – capable of investing in infrastructure and providing technical expertise for service operations -, have the ability to enable innovative contract arrangements. This could lead to modernization of this service, among others, through the installation of LED bulbs and the implementation of automated control centers for efficient network maintenance.

Concessionaire compensation is linked to its performance in service provision and it assumes part of the risks provided in contracts and listed in Article 6, paragraph 1 of Law no. 11.079/2004.<sup>cccv</sup> In some ways, PPP contracts may allow the Public Power to diminish certain operational risks involved in the implementation of smart street lighting networks, as the responsibility for financing, equipping and maintaining the system in a perfect state of functionality will be relegated to a private partner, who will fulfill the services rendered, according to predetermined quality standards in the partner contract.<sup>cccvi</sup>

By early 2017, there were already more than 100 PPP projects initiated by cities with the objective of implementing smart street lighting systems. All of them were modeled on a species of administrative concession, with an average investment of approximately 273 million reais per PPP contract for smart public lighting management.<sup>cccvii</sup>

An interesting observation is that three projects establish consortium initiatives, with one PPP contract for more than one city, as provided by article 241 of the Federal Constitution and Law no. 11.107/2005.<sup>cccviii</sup> This contract arrangement is useful (i) in making the smart street lighting project less expensive for the cities, considering that costs and investments made by the concessionaire are distributed among the participating cities; and (ii) in maximizing the efficiency of the PPP contract, as different cities are merged in one single contractual standpoint.<sup>cccix</sup> Likewise, PPP smart street lighting contracts is no simple task for mid-sized or small cities, as these contracts



have intricacies and their clauses and conditions establish a connection for up to 35 years (Article 5, II, Law no. 11.079/2004).

Among the PPP smart lighting projects, a São Paulo project stands out for being among the largest, and for facing numerous obstacles that resulted in the suspension of the project. Aimed at the modernization, optimization and expansion of the entire lighting network of the city of São Paulo, COSIP was the source of funding. The main goals were replacing traditional lighting with LED bulbs with controllers (a device responsible for the communication between the light fixture and the Operational Control Center) and the creation of new lighting points.<sup>cccxx</sup>

The contract was hindered by repeated decisions in the city's Court of Audit, with the support of the State of São Paulo Court of Law.<sup>cccxxi</sup> The first issue was caused by technical inconsistencies in the public notice, such as the divergence between the text and the version of the draft sent for public consultation.<sup>cccxxii</sup> The second issue emerged due to opening of envelopes containing proposals presented by competing companies. The winning consortium filed an appeal before the Municipal Court of Audit due to the evaluation commission not having accepted the guarantees it had offered. Note that the obstacles to establish the PPP were not specifically related to the public lighting sector nor to the financing with COSIP funds.<sup>cccxxiii</sup>

Therefore, this experience shows the relevance of financial guarantees presented by the cities to potential partners in the publication of calls for bids and in the establishment of concession contract.<sup>cccxxiv</sup>

Despite this experience, the implementation of PPPs in public lighting is adequate given the shortage of financial resources and organization of the cities and draws on the expertise of the private market in the area. In any event, the implementation must carefully observe the requirements of specific legislation in order to avoid obstacles due to Court decisions.

#### g) Privacy in Smart Public Lighting

Public lighting is among the main segments of municipal infrastructure and has been undergoing modernization through the installation of LED bulbs, recognized for their energy efficiency. This modern public lighting infrastructure will soon feature technological mechanisms, like sensors and audiovisual devices that collect data to exercise their functions. Authorities often use lighting sensors, surveillance cameras and noise-capturing sensors to detect suspicious activities in local areas.<sup>cccxxv\_cccxxvi</sup>

Although adding such equipment to the network offers opportunities including reduced electricity consumption<sup>cccxxvii</sup> and efficient management of urban traffic, its data-collecting capability raises concerns regarding the privacy of individuals. In 2014, The New York Times revealed privacy issues related to data collected by sensors and cameras installed in the smart lighting system of Newark-Liberty International Airport, just outside New York City. The data, in the hands of the Port Authority administration, could indicate individual behavioral patterns of individuals who had been at the airport.<sup>cccxxviii</sup>

Furthermore, the interconnection between public lighting and various devices connected to the Internet can make the public lighting infrastructure vulnerable to cyber-attacks, as occurs with

smart electricity meters.<sup>cccxix</sup> Therefore, it is important for the Public Power to act in a collaborative way to protect the security of information contained in this public service structure, by encouraging private entities who manufacture and distribute these new devices to adopt standards of conduct within the legislative framework on personal data privacy and protection.<sup>ccxxx</sup>

In conclusion, the same recommendations made for smart meters are applicable to the context of smart public lighting, among which are (i) the need to issue a specific law to protect personal data, capable of consolidating the still sparse legal understanding on the topic and to determine reach of protection of data collected by the public sector; (ii) not needing to obtain previous consent for private data crucial to the provision of essential public services; (iii) compliance with the purposes for which the data is collected, enabling data to be used only for those specific purposes; (iv) the existence of opt-out systems that enable individuals to choose not to have their personal data used for purposes different from the provision of essential public services, with no penalties applied for this choice; and (v) the adoption of different data anonymization and aggregation techniques, also in cases of data collected in public spaces – when used for purposes other than the original; (v) a normative determination that establishes that data cannot be shared with third parties, except when anonymized or with previous free, express and informed consent; (vi) the determination that data cannot be shared with any other governmental body (such as the Brazilian Tax Authority, police authorities, among others) except in the case of a previous court order authorizing this.

#### 7.5. Urban Mobility

Mobility consists of the ability of persons and assets to circulate in the urban environment, and is an important element for quality of life and to access essential services in cities. It also directly influences social and economic development. The quality of mobility directly reflects on how citizens experience the city, as security and travel times may present either obstacles or may ease access to work, recreational centers and public services in general.

Brazil's urban centers currently face major traffic congestion, insufficient public transportation and high levels of traffic accidents. Among the challenges to improve the mobility of assets and people in the urban space, developed in the pages that follow, are<sup>ccxxxi</sup>:

- Reduction of travel times and improvement of citizens' traffic experience;
- Improvement in the management of public transportation, especially to promote efficiency, safety and quality to the service;
- Prioritization of public transportation over private vehicles;
- Integration of different types of transportation;
- Encouragement of non-motorized mobility (pedestrians and bicycles); and
- Adoption of measures to ensure universal accessibility.

As will be presented below, the adoption of IoT devices by traffic and public transportation equipment and infrastructure may help with the mentioned challenges and, consequently, with the improvement of citizens' experiences in the cities.<sup>cccxxxii</sup> There are numerous possibilities of mobility IoT solutions, such as the use of cameras and sensors to collect information that enables real-time traffic planning. However, the analysis of the regulatory framework for mobility will be restricted to two aspects, consisting of: (a) central and adaptable traffic control; and (b) monitoring of public transportation mobility.

#### a) Urban Mobility Competencies

The design and implementation of traffic and transportation policies with IoT technologies must consider that the legislative competency is exclusive to the Union, but that States can legislate with express authorization, as provided for in Complementary Law (Article 22, subsection XI, single paragraph, of the Federal Constitution).<sup>cccxxxiii</sup>

Regarding traffic, other federal entities are authorized to establish public policies as long as related to traffic security, including actions in education, engineering, traffic inspection and other activities that promote the right to efficient urban mobility and are provided in the law (Articles 23, XII and 144, paragraph 10, I and II of the FC).<sup>cccxxxiv</sup>

On the other hand, transportation is more specific in terms of its competencies. The Union is responsible for establishing basic guidelines for urban development and for legislating on national transportation policies (Article 22, IX and XX of the FC). States regulate intermunicipal transportation services<sup>cccxxxv\_cccxxxvi</sup> and cities organize and provide public collective transportation service within urban limits (Article 30, V). Therefore, regulation and inspection of transportation services are exercised jointly by all federal spheres, depending on which territorial area the transportation occurs.

Therefore, the regulation on the use of IoT devices to promote smart mobility must observe federal, state and municipal traffic and transportation safety laws. Within this framework, noteworthy items are the Brazilian Traffic Code (Law no. 9.503/1997), norms established by the National Traffic Council – CONTRAN, the National Urban Mobility Policy (Law no. 12.587/2012) and city norms on mobility and transportation (provided in a Master Plan or in a Mobility Plan).

#### b) Traffic: Centralized and Adaptable Control

##### Opportunities Created by IoT solutions

Systems already utilized by the Public Administration to control traffic, such as video monitors<sup>cccxxxvii</sup> and radars, may be enhanced by new technologies such as OCR (Optical Character Recognition), a technology capable of automatically recognizing vehicle license plates,<sup>cccxxxviii</sup> and sensors installed in bicycle lanes and sidewalks to measure pedestrian flow or to produce energy.<sup>cccxxxix</sup> To offer additional support to traffic control, IoT solutions must be interconnected with a data processing center, enabling the identification of traffic conditions and the promotion of actions to improve the flow of vehicles, cyclists and pedestrians.<sup>cccxl</sup>

Among the opportunities created by the use of these data collection and processing devices is the better timing for traffic lights through redirecting traffic in real time, optimizing circulation of pedestrians, cars and cyclists. One simple command from the control center will be able to change an intersection's wait time due to traffic.<sup>cccxi-cccxliii</sup>

It will also be possible to offer real-time information on local traffic to the population.<sup>cccxliv</sup> This service may be improved by data from social media and platforms that enable the monitoring of user conditions. An example is the partnership between Waze and São Paulo City Hall, to provide information on broken traffic lights to the Public Power. According to the Traffic Engineering Company (known as "CET"), this program of public-private cooperation has the power to reduce the response time to problems detected by the traffic control system.<sup>cccxliv</sup> In a similar way, the Rio Operations Center (known as "COR"), in the city of Rio de Janeiro, uses the application's platform to inform citizens of scheduled interventions or other types of occurrences that may affect traffic.<sup>cccxliv</sup>

#### Regulation of Traffic Control Equipment

Considering the Union's private jurisdiction over traffic, in 1997 Law no. 9.503/1997 was issued (the Brazilian Traffic Code – Traffic Code), addressing the National Traffic System, the rules of conduct for traffic and the infractions applicable to their noncompliance. The inclusion of new technologies to the traffic management system must therefore consider the norms and competencies established by the Traffic Code.

The regulation of the Traffic Code is a competency of the National Traffic Council – CONTRAN, a regulatory and advisory entity of the National Traffic System (article 12), and the modernization of traffic infrastructure must be supported and regulated by it. The Traffic Code forbids the use of signaling devices that are not addressed by traffic legislation, and CONTRAN has the power to allow the experimental and temporary use of different types of signaling devices (Article 80, caput and paragraph 2).

CONTRAN is also responsible for organizing and developing manuals and norms related to the implementation of traffic equipment it approves (Article 12, XIX of the Traffic Code). For this reason, the body has issued norms to regulate the use of certain devices, such as video monitoring systems, speed meters and vehicle identification equipment.

The modernization and integration of technological devices that monitor urban traffic flow are also supported by Federal Law no.12.587/2012 (National Mobility Policy), which regulates article 182 of the Federal Constitution and establishes general norms for urban mobility. Among other things, it provides the integration of cities' traffic networks (Article 1), efficiency and security in the transport of people (Article 5, IV, VI and XI) and incentive for scientific-technological development (Article 6, V).<sup>cccxlvi</sup> It also prioritizes the use of non-motorized vehicles and public transportation services over private motorized vehicles (Article 6, II), which may be enhanced through the use of IoT devices.

Despite federal traffic regulations, cities play an important role as their bodies and entities are responsible for implementing, maintaining and operating traffic control equipment (Article 24, III of the Traffic Code).<sup>cccxlvi</sup> As detailed ahead, municipal capacities must be provided in specific regulation, such as the city of São Paulo's municipal mobility master plan (Law no.

16.050/2014),<sup>cccxlvi</sup> which provides for activities and guidelines such as the increase in traffic light waiting time in places with high pedestrian flow (Article 222, VIII) and the development of traffic light communication plans with controllers to improve traffic flow by prioritizing collective passenger transportation (Article 245, I, “c”).

Considering this scenario, the Pedestrian Statute (Municipal Law no. 16.673/2017),<sup>cccxlix</sup> was recently issued and ensures pedestrians the possibility of benefiting from smart traffic signs equipped with timers.

The use of electronic devices, including audiovisual equipment, to verify traffic infractions is provided by Article 280, paragraph 2 of the Brazil Transportation Code and has been regulated by CONTRAN Resolutions no. 471/2013 and 532/2015.<sup>ccccli</sup> Traffic agents are responsible for sanctioning drivers and vehicles with infractions detected online through these systems, but traffic inspection through monitoring cameras may only occur in public streets marked by signage for this purpose (Articles 2 and 3 of Resolution no. 471). By allowing cities to use images captured by cameras to prove infractions, these Resolutions have enabled a series of other municipal initiatives, such as the Smart City project city in Nova Friburgo in the state of Rio de Janeiro, which has installed security cameras through the urban area with the purpose of making the traffic infraction system more efficient.<sup>ccccli</sup>

On the other hand, radars, devices used to measure the speed of automotive vehicles, are regulated by CONTRAN Resolution no. 396/2011.<sup>cccclii</sup> This regulation determines the competency of INMETRO to approve and periodically inspect if radar models are compliant to current metrology legislation (Article 3, I to III). The implementation of these devices is the responsibility of the authority in charge of the street where the devices will be located (Article 4), so, when located in the streets of a determined city, local municipalities are responsible for stipulating their location, installation and operation.

Concerning vehicle identification, CONTRAN manages the National Automatic Vehicle Identification System (SINIAV), based on radiofrequency technology, under Article 1 of Resolution no. 412/2012.<sup>ccccliii</sup> According to related regulations, all vehicles circulating in the country must have an electronic identification chip (Articles 1 and 2 of Resolution no. 537/2015).<sup>ccccliv-cccclv</sup> The information obtained through these devices is used by public organs and entities part of SINIAV, for purposes and competencies attributed to the system, observing the confidentiality of the information (Article 7, Resolution no. 412/2012).

However, the system has been facing obstacles related to financing, as the Resolutions do not determine who is responsible for costs, and actors in the traffic system indicate no specific budget to achieve the objectives.<sup>cccclvi</sup> Although attempts to implement SINIAV have been started with the enactment of CONTRAN Resolution no. 212/2006, the system is still inactive, as only the state of Roraima has conducted a bid to purchase equipment.<sup>cccclvii</sup>

Therefore, the modernization of traffic equipment through IoT solutions must observe federal legislation regulated by CONTRAN Resolutions and municipal legislation especially in cases of possible mobility and master plans. CONTRAN resolutions are aligned with the new technology

trends, and the main challenge to implement IoT in mobility is the inclusion of technological changes in the local legislation.

#### c) Transportation: Circulation Monitoring and Maintenance Based on Conditions

##### Opportunities Created by IoT Solutions

Urban transportation has been recently included as a constitutional civil right of Brazilian citizens (by Constitutional Amendment no. 90/2015) and represents one of the most important pillars of individual life quality indexes.<sup>ccclviii</sup> However, the provision of this public service still represents a significant challenge to the Public Administration and still depends on quality and safety improvements. Among the causes of intense traffic situations observed in large Brazilian cities<sup>ccclix</sup> are an insufficient infrastructure to satisfactorily service the entire city territory,<sup>ccclx</sup> a model that prioritizes private cars and poor maintenance of public transportation services.

In this context, the use of IoT technologies has great potential to contribute to better planning of the urban public transportation system, through the use of a group of sensors connected to transport units, capable of monitoring user flow, public streets traffic conditions, as well as the location of public transportation vehicles – the last one especially through the use of location sensors with GPS (Global Positioning System).<sup>ccclxi\_ccclxii</sup> This is the case for the city of Curitiba, which has been advancing in the development of technological solutions to connect and accompany public equipment in real time, such as the municipal bus and public health system vehicles.<sup>ccclxiii</sup>

Considering that these sensors collect a massive amount of data, big data and analytics, they are important tools to optimize the user experience, creating benefits to the system's reliability.<sup>ccclxiv</sup> This happens because the processing and crossing of data collected by these sensors help to provide information on, for example: (i) arrival and departure times of vehicles and the routes they travel; (ii) which route is the best option in a particular time of day; (iii) which time of day has heaviest movement for each type of transportation; and (iv) which type or combination of transportation is ideal for a determined itinerary.<sup>ccclxv</sup> The Public Power could use the collected data to improve the effectiveness in the planning of activities, recognizing population displacement behavioral changes more quickly and anticipating construction works and the availability of material and human resources to execute them.

Data generated by the circulation of transportation units also facilitates the execution of audits of concession contracts of public transportation services, since they allow a more certain inspection of the compliance to the speeds determined by the concession entity.<sup>ccclxvi\_ccclxvii</sup> It would also be possible, for example, to monitor supply to users during hours of lower demand. Also, the use of sensors in buses and trains enables more efficient maintenance and updates to the transportation infrastructure, executed as demanded and at times that would not affect its use by citizens.<sup>ccclxviii</sup>

##### Regulation of Urban Transportation Services

Just like traffic, transportation is also regulated by the Brazilian Transportation Code, but is addressed in more depth by the City Statute (Law no. 10.257/2001) and the National Urban Mobility Policy (Law no. 12.587/2012). The City Statute establishes the offering and guarantee of access to

transportation (Article 2, I and V) as urban policy guidelines, and establishes that master plans of cities with more than 500,000 inhabitants are required to have an integrated urban transportation plan (Article 41, paragraph 2). It also establishes that the Union is responsible for determining guidelines for transportation and urban mobility, which substantiated the creation of the National Urban Mobility Policy.

The issuing of the abovementioned legislation is considered an advance from an institutional point of view, as this forms a regulatory framework for the formulation and execution of public policies for the urban environment and for the improvement of traffic and public transportation services. However, they must be complemented by an integrated management of the State and Cities and by investments in infrastructure.<sup>ccclxix</sup>

In this context, the National Urban Mobility Policy attributed to the Union the responsibility for providing technical and financial assistance to other federal entities and for fostering scientific and technological development in mobility (Article 16, I and VI). It also attributed to it the prerogative to issue standards that facilitate cooperation between federal entities, a relevant role in a scenario of shared regulatory and administrative functions.

The States were designated with attributions related to the proposition of a taxation policy, specifically for the implementation of the National Mobility Policy (Article 17, II), and to the Cities, the adequate execution of the Mobility Policy, through the planning and provision of collective public transportation services, in direct or indirect way or through associated administration (Article 18). Therefore, the cities have a relevant role in the regulation and execution of transportation services, especially through master plans, when their implementation is mandatory.<sup>ccclxx</sup> Thus, Master Plans of cities such as Curitiba, Rio de Janeiro, Salvador and São Paulo<sup>ccclxxi</sup> have chapters specifically dedicated to mobility policy, all of them determining a mobility network that prioritizes public transportation and non-motorized means of transport. In the same way, these regulations have legal devices that stimulate improved technology levels both in the management of collective public transportation systems – in Article 217 of the Master Plan of Rio de Janeiro provides the implementation of smart technologies in the integrated transportation network of the city -, and in traffic control, as provided in Article 243 of the Master Plan of Salvador, which determines the use of technological strategies in signaling and traffic security devices.

The Mobility Policy also determines that public transportation system users have the right to free and accessible information on routes, times, service tariffs and interaction with other types of transportation (Article 14), a context in which the described IoT solutions may serve as an efficient instrument for mobility rights.

Moreover, the enhanced technology within public transportation, such as radars capable of identifying the flow and location of users and vehicles, may help to achieve the principles of the urban policy.<sup>ccclxxii</sup> These are mechanisms to improve efficiency in service provision by providing information to users on the location of a determined vehicle and also by enabling the optimization of quality equipment and public transportation offerings (Article 2, I and II, of the City Statute) and the improvement of people and cargo mobility around the city (Article 1, caput, of the Mobility Policy).

In this scenario, the implementation of IoT technology must consider that the Union is responsible for offering financial assistance to the cities for the technological improvement of their mobility structures (Article 16, I, of the Mobility Policy), which use federal financing lines to fund the installation of different types of sensors suitable to transportation units and circulation areas. The States may equally contribute to the financing system, as they are responsible for implementing tax changes and tax incentives to enable the adoption of these technologies (Article 17, II, of the Policy).

In conclusion, different federal spheres must cooperate in jointly managing compliance to the public transportation service contracts. Considering that the Union, States and Cities all have roles in the provision of urban transportation and management of mobility, federal standards to coordinate and foster this cooperation is essential. The modernization of urban transportation services must equally observe national guidelines and municipal regulations. In addition, IoT projects related to public transportation may be stimulated through financial support provided by the Union and the States.

#### d) Brief Notes on Privacy, Information Security and Data Use

The installation of technological information and monitoring devices added to the traditional control traffic systems and to urban mobility infrastructure results in a significant increase in personal data collection and analysis. As previously mentioned, data collection and analysis are relevant to improve public transportation services and activities directed at improved quality in the mobility of assets and people. This improvement is based on immediate data aggregation and analysis, capable of better utilizing technological, personal and financial resources. Moreover, databases of public traffic bodies may be integrated with databases of other public or private services, further enhancing existing solutions. Groups of traffic data, for example, may be combined with data collected by devices added to the public lighting infrastructure, creating a source of information to the Public Power that may lead to more efficient decision-making in public services.

Updated and robust databases create generate a great deal of criticism regarding the security of information and the privacy of citizens' personal data.<sup>ccclxxiii</sup> As sensors, cameras and other devices used in traffic may use wireless or wired connectivity, the mobility data collection system may be vulnerable to security failures. This type of situation is often reported in the media, such as the attack on the San Francisco transportation system's computer network in 2016,<sup>ccclxxiv</sup> and in the recent case of the ransomware Wanna Cry in Germany's train networks.<sup>ccclxxv</sup> In this context, the partial report "Product 8: Expansion of Verticals – Cities", of September 2017, states the importance of implementing security mechanisms against intentional signal interference (anti-jamming) in order to avoid cyber-attacks.

Also, the use of such devices may identify individuals, either by the direct collection of personal data or through crossing of certain data from external sources. As examples of databases formed by traffic bodies, one may mention the databases of the systems and subsystems of Denatran (the National Traffic Department), which contain data such as drivers' licenses, infractions and good standing of vehicles before the traffic bodies. The access to this database is regulated by Denatran Ordinance no. 15/2016<sup>ccclxxvi</sup> and is provided only to public bodies and private entities, although data is commercialized through the service provided by the Federal Data Processing Service – Serpro, a public company.<sup>ccclxxvii</sup>



In this context, we reiterate recommendations previously addressed on the topic of urban privacy. Above all, we point out the need to issue a specific law for personal data protection that establishes parameters for collection, handling and sharing of personal data collected within the context of modernization actions of the public administration. Note that the recommendation is based on legislation still awaiting approval in National Congress, as the provisions of the Internet Framework serve the proposed purposes.

However, given the current sparse legislative context, it is extremely relevant to adopt measures capable of minimizing risks related to the identification of individuals and a possible violation of privacy, among which we can highlight:

- Compliance with the principle of purpose for use of collected data;
- Obtaining free, express and informed consent from users – especially when data will be submitted to any anonymization processes -, for any other use attributed to the collected personal data other than the original purpose of providing an essential public service, as described in the Internet Framework;
- Availability of opt-out mechanisms to users who may choose not to have their personal data used for purposes other than the strict provision of essential public services, as a means to enable control over possible use of their data;
- Obtaining of previous, free, express and informed consent to share data with third parties, except in cases of public interest provided in the law or by court order,<sup>ccclxxviii</sup>
- Use of different data anonymization and aggregation techniques, such as cryptography and blockchain<sup>ccclxxix</sup> technology, especially when the use of personal data is different from its original purpose.

Complying with these measures is very important, especially considering that the data collected for provision of public services – which may be considered a fundamental right of citizens. In this context, partnerships established by governmental bodies that involve data collection for private entities must comply with specific legislation on public contracts to favor free competition and establish strict rules for personal data collection. Still, the refusal to consent or use of opt-out mechanisms must not preclude the citizen from using public services.

Beyond information security and collected data privacy related to traffic and public transportation policies, the best practice is that IoT solutions – whenever possible – be based on open standards, free software or open source, and, in the case of open data, API. Free software or open source is a computer program built in a free and collaborative way, possible to use if copied, changed or redistributed without the need of permission from its original creator.<sup>ccclxxx</sup> It is also essential for the free software to have a free source code, accessible to third parties and non-exclusive to authors and owners.<sup>ccclxxxi</sup>

The adoption of this type of software by the Public Administration attends to the constitutional principle of efficiency in the public sector (Article 37 of the Federal Constitution) and may prevent a monopoly in software contracts for governmental use. Beyond this, it avoids the

“lock-in” effect, a result of technical difficulties caused by software migrations or data transfers previously collected by and stored within the software of a determined supplier.

Among the advantages of governmental use of a free software are (i) being free for government and citizen use; (ii) the possibility of personalizing the software according to the needs of the provided public service; (iii) public body and user autonomy, independence from contracting software owned by a determined supplier; and (iv) greater system security, as its collaborative format allows constant contributions from third parties in identification and improvement of failures.

Some Brazilian cities already use free software in their computer programs and systems. One example is São Carlos, which issued Law no. 12.883 in 2001, stipulating that City Hall must prioritize the use of programs with open, restriction- and ownership-free source codes.<sup>ccclxxxii</sup> The Municipal Secretary of Transportation of the City of São Paulo also issued in 2015 a notice to contract free software in order to, among other objectives, automate sanctions and infractions processing and public transportation quality analysis.<sup>ccclxxxiii</sup> However, the use of this type of software relies on the initiative of the public manager, as there is no local legislation on the topic, and the Federal Public Administration has not greatly promoted development of a free software policy in recent years.<sup>ccclxxxiv</sup>

The API is a group of programming standards that enables the creation of new applications. Its adoption by public bodies allows external developers to contribute to the development or improvement of applications capable of communicating with governmental databases.<sup>ccclxxxv</sup> Open data, in turn, is the name given to data disclosed on the Internet, in an updated, open and reusable format. In this context, the use of API for open government data allows third parties to use updated public data to create new technology solutions in collaboration with public services.

Even if public bodies must make an investment to disclose their databases in a property-free, machine-legible format, the solution has the potential of enabling the development of IoT applications based on public updated data. For example, data collected by traffic sensors or by GPS installed in buses, and data available in public databases may be transferred to mobile device applications such as cellphones, enabling passengers to reduce their wait times. A better estimate of departure and arrival times may also affect a passenger’s choice to use collective passenger transport or combination of transportation models instead of an individual car.<sup>ccclxxxvi</sup>

Considering the benefits offered by API for open data, the federal government has an open-data platform for different Federal Public Administration bodies.<sup>ccclxxxvii</sup> Likewise, the city of São Paulo also has a platform for developers, in which it discloses databases related to different areas of the city.<sup>ccclxxxviii</sup> However, the adoption of open standards is not yet widely disseminated within public bodies, hindering improvement of public transportation and traffic services through API use.

Finally, we include an important note on artificial intelligence and automated decisions made by algorithms. As smart city and IoT applications become more common, they also become cognitive. In other words, their operations become integrated with “smart” decision making systems, based on algorithms or even on artificial intelligence applications.

In the public sector, this type of integration among IoT, algorithms and artificial intelligence requires special attention from a public policy and regulatory point of view. In the words of Harvard professor Lawrence Lessig, in his 1999 book *Code: and Other Laws of Cyberspace*: “the code is the law”.

Lessig highlighted that computer programs (“codes”) will become increasingly important, as they embed themselves in rules that direct decisions for a great number of persons on a daily basis.

To ensure that an algorithm is being used appropriately by the public sector, with no external interferences and attending to the principles that regulate public administration, it is fundamental for both the code and the hardware to be known, transparent and auditable.

This concern clearly signals a new paradigm for public transparency. Every and any public function mediated by a “code” must attend to the transparency and accountability requirements when employed by the public power. In example, both code and embedded hardware must be transparent, auditable, preferably open to citizens’ analysis, including the maintenance and updating processes.

In his pragmatic book, Lessig mentioned that one of the challenges to embed norms and codes is a function of the fact the few people understand the language. This opacity could serve as cover for corruption. Therefore, it is fundamental for any automated decision-making by the Public Power, be it through algorithms, artificial intelligence or other types of analysis, to comply with the general principles that regulate it, among which are impartiality (the rejection of analysis based on stereotypes or prejudice), publicity (transparency and audibility) and efficiency, as well as right to appeal decisions made within the scope of the public administration.

This concern has already been presented before National Congress, within a Bill that specifically addresses it. We consider Bill no. 8.503 of 2017<sup>ccclxxxix</sup> to be positive, adequate, and a portion of the wording follows below:

#### Bill 8.503/2017

Alters Law no. 12.527, of November 18, 2011 (Access to Information Law), expressing the right to obtain information related to the acquisition and functioning of software, hardware and codes in public functions and makes the provision of algorithm source codes used to distribute cases within the Judicial Power mandatory. The National Congress decrees: Article 1 of Law 12.527, of November 18, 2011, becomes effective with the following increments:

#### *Article 7*

*VIII – information and technical detailing of the creation, acquisition, configuration and functioning of software, hardware and mediating codes of any public function (NR)*

#### *Article 8 paragraph 3*

*IX – In cases of Judiciary Power bodies, disclose the auditable source codes of any employed algorithm or automated system, including those for distribution, as well as the parameters and statistics related to their functioning. (NR) Article 2 This Law becomes effective on the date of its publication.*

## 7.6. Regulatory Aspects of Contracting Information Technology and Communication Solutions by the Public Administration

### a) Introduction

For this topic, we will address the general aspects involved in contracting Information Technology and Communication (ITC) goods and services by the Public Power, such as machines; equipment and devices based on digital technology (hardware); various electronic components; machine programs, equipment and devices (software); and technical services related to those assets.

To do so, we have identified the applicable standards that regulate contracting of ITC solutions by the Public Administration, which may also be used as a parameter by municipal bodies in the absence of local regulation. Next, we present an example of ITC hiring by the Federal Public Administration, in this case, case cloud computing services. Finally, we address the main challenges faced by public entities for contracting ITC solutions and outline the discussion regarding possible relaxing and improving of current regulation.

### b) Regulatory Panorama of Public Administration ITC Contracting

Contracting of ITC must be guided by the general bidding procedures provided for by Laws no. 8.666/1993 (Procurement Law) and no. 10.520/2002 (Reverse Auction Law) and in their regulatory Decrees no. 5.450/2005 and no. 7.892/2013.<sup>cccxc</sup>

In the federal scope, contracting must also follow specific rules for ITC solution acquisitions, described in the following pages.

- Decree no. 8.135/2013 and Inter-ministerial Ordinance no. 141/2014

Federal Decree no. 8.135/2013 establishes that every data communication within the Federal Public Administration must occur through telecommunication networks and information technology services provided by bodies or entities of the federal public administration itself. However, Inter-ministerial Ordinance no. 141/2014, which regulates the Decree, makes an exception by establishing that when the public institution is not capable of adequately providing the IT service, it may be provided by private entities (Article 7). In these cases, a call for bids is mandatory, while in cases of direct solution provision by the Public Power, a bid is not required (Article 2 of Decree no. 8.135).<sup>cccxcii</sup>

Related actions adopted by the Ministry of Planning, Development and Management and by the Union's Court of Audit<sup>cccxcii</sup> indicate that both have been applying a broad interpretation of Article 7 of the Ordinance, so as to ease contracting of private entities for ITC solutions. This may be motivated by the current inability of Federal Public Administration bodies to offer ITC solutions required by the government.

- Decree no. 7.174/2010

This regulates contracting of computer and automation goods and services by the Federal Public Administration. It determines that the acquisition must be followed by the development of planning, through a basic project or terms of reference, provided that such documents do not favor a specific supplier (Article 2). However, its rules do allow for preference for Brazilian technology products and services (Article 5), within the determination of Law no. 8.248/1991.<sup>cccxciii</sup>

The Decree also determines that, when contracting computer and automation goods and services, the Administration must adopt the “lowest price” or “technique and price” bidding models (Articles 9 and 10) – authorized in Article 45, paragraph 4 of Law no. 8.666/1993. The “lowest price” bid is exclusive to the acquisition of computer and automation goods and services that are considered common services provided by various suppliers, and will adopt the “reverse auction” model. On the other hand, the “technique and price” bid is used for computer and automation goods and services that are predominantly intellectual, as their characteristics require individual consideration.

- SLTI/MPOG Normative Instruction no. 04/2014

Issued by the Ministry of Planning, this normative ruling specifically addresses the contracting of ITC solutions by bodies and entities in the Information Technology Resources Administration System (known as “SISP”), a system created to manage the information technology resources by direct, autarchic and foundational administration of the Federal Executive Power.<sup>cccxciv</sup>

In general, the Instruction expressly forbids that (i) contracting involve more than one ITC solution per contract and that (ii) aspects of information security management are addressed (Article 5). SISP member entities must follow three steps for every contract: contract planning,<sup>cccxcv</sup> vendor selection,<sup>cccxcvi</sup> and contract management, which the Administration must monitor ensuring the adequate provision and supply of goods and services (Article 8).

- Information Security Standards issued by GSI

According to Decree no. 3.505/2000, the Institutional Security Cabinet of the Presidency of the Republic has the competence of regulating information security issues within the Federal Public Administration.<sup>cccxcvii</sup>

The Cabinet has issued normative instructions and several additional standards establishing information security standards for ITC services provided to federal entities.<sup>cccxcviii</sup> The norms issued are considered by the Court of Audit as mandatory for the Federal Public Administration.<sup>cccxcix</sup>

In conclusion, even with the enactment of this regulatory scenario for contracting of ITC products and services by the Federal Public Administration, Brazilian cities must comply with both these regulations and local ones. Federal norms can be used as a parameter for contracting when there are no specific related norms within the municipal sphere, provided that the position of the city’s competent Court of Audit is considered – as State and Municipal Courts of Audit may have different understandings (which is the case of the cities of São Paulo and Rio de Janeiro) and eventual Court of Audit decisions.

## Aspects of Contracting Cloud Computing

Among the recent activities of public bodies in relation to ITC solution contracting, the 2017 Court of Audit bid to hire cloud computing services stands out.<sup>cd</sup> In the adopted Terms of Reference, the Court chose to hire a specific type of cloud computing service, the cloud broker (or cloud service integrator).<sup>cdi</sup>

Even if such Terms of Reference are not binding to other Public Administration bodies, they may serve as a reference for future bids. After holding a public consultation on “Terms of Reference – Cloud Computing Service” in 2017, the Ministry of Planning adopted a contracting method through an integrator used by the Court of Audit.<sup>cdii</sup>

In addition to the group of norms related to hiring the previously described ITC services, the Public Administration must also comply with: (i) Institutional Security Cabinet additional standards no. 4 through 19; (ii) MP/STI Ordinance no. 20/2016 of the Ministry of Planning<sup>cdiii</sup> focusing on its annex that contains general guidelines and good practices<sup>cdiv</sup>; and (iii) decision no. 1.739 of 2015, issued by the Union’s Court of Audit, as well as its Annex I.<sup>cdv</sup>

Among the recommendations and requirements established by these regulations is, first, a preference for implementing hybrid cloud services<sup>cdvi</sup> for Ministry of Planning contracts, provided it does not place national security at risk, according to Ordinance no. 20/2016.

Second, the Ordinance mandates the Administration to require, in its cloud computing service contracts, that data or information, including security copies (backup), are stored in servers located in Brazil.

Third, the Ordinance’s general guidelines establish that public bodies must ensure through contract clauses that the hired cloud computing service allows the migration of data and applications and that the information of the hiring body is available for migration in an adequate period and with no additional cost, in order to ensure business continuity and enable contractual transition (item 11).<sup>cdvii</sup>

Fourth, the Ordinance also determines that the Administration must ensure the confidentiality of information or data in its cloud computing service contracts, prohibiting the service provider from using it or transferring it to third parties without proper authorization from the public bodies (item 12).<sup>cdviii</sup>

Fifth, according to Institutional Security Cabinet Complementary Standard no. 14/2012, the Administration must require the cloud computing service provider to guarantee the prevailing of Brazilian law during service provision (item 5.2.2).<sup>cdix</sup> In the opinion of the Court of Audit, although this norm does not expressly prohibit contracting of cloud computing services that have servers located in other countries, it may limit the Administration in practice from contracting cloud computing services that have servers physically located in other countries.<sup>cdx</sup>

Finally, the Court recommends cloud computing service providers be required to implement security methods to store and transfer data, such as the use of encryption (compatible with the level

of confidentiality of the stored information) and Virtual Private Networks (VPN). As for cloud computing API, the understanding is that it must be developed in compliance with security standards used by the market, including strict user authentication and access control mechanisms.

#### c) Mapping of the Current Debate on Public Administration Contracting of ICT solutions

##### Legislative Competence on Bidding

With an overview of the legislation for Information and Communication Technologies contracting public bodies presented, in this section we turn to a partial mapping of obstacles faced by the public manager in conducting those procedures.<sup>cdxi</sup>

Initially, the main obstacles faced at the local level for contracting ICT solutions are closely related to the distribution of legislative competencies on bids. As determined by Article 22, XXVII of the Federal Constitution, the Union has competency to issue general norms on public contracts, and other federal entities are responsible for addressing local aspects.

As is well known, general rules address interests not restricted to the local scope of federative entities, that is, they address the general interests of all of them. One possible delineation is that modalities (e.g. open “auction”-style model known as “pregão” and invitations to bid) and types (e.g. “lowest price” or “technique and price”) of bidding<sup>cdxii</sup> should not be issued by states or cities, since rules issued by these entities must not address general interests (only local) and must not go against constitutional directives such as isonomy between bidders (Article 37, XXI of the FC).

In a recent decision, the Federal Supreme Court (“STF”) confirmed the constitutionality of a state law that establishes the abstract preference for free software, since it is a matter of “regular” legislative competency and does not exclude potential bidders from the universe of contracts with the Public Power.<sup>cdxiii</sup> On the other hand, the unconstitutionality of the state law was confirmed in a previous case, as it caused competitive restrictions to companies in bidding processes. By conflicting with the general forecast of isonomy between competitors, the law would extrapolate the additional legislative competency endowed to the States.<sup>cdxiv\_cdxv</sup>

In short, one can affirm that the establishment of bidding procedures that restrict the way in which it will be executed is authorized to the Cities, States and the Federal District (Article 24, XI, of the FC). However, this does not mean that it is authorized for local norms to establish new modalities or selection preference or to suppress phases of the bidding process. After all, public procurement procedures are largely defined within the federal level, and not very flexible to changes according to local characteristics. This scenario overly limits the possibilities of flexibility and adequacy of bidding processes to the specifics of ICT.

Nevertheless, some of the obstacles faced will be further discussed below. For now, we emphasize that, among the aspects that can be regulated locally, are: (i) the inclusion of additional aspects related to the minimum content of auction notices; and (ii) the definition of figures and deadlines included in auction notices.

##### Institutional and Technical Capacity of Cities

Among the obstacles faced by the cities in developing an ICT contracting process is the lack of institutional capacity to (i) identify the demand for these products; and (ii) develop a specific project and auction notice for their demand.<sup>cdxvi</sup> Unlike other essential products for public management, new technologies are made available in the market at all times or can be designed specifically for the needs of a particular public body or entity.

The forecast of demand requires technical capacity to evaluate the launch of new products and the technical specifics of the desired acquisition. The development of a bidding process also requires knowledge from the manager to identify and justify the need for a particular product, as well as to design an auction notice capable of selecting the best product available for its needs.<sup>cdxvii</sup> However, sometimes managers and staff of the Administration are not familiar with basic technical concepts and characteristics of technological products.

Among the challenges faced in the design of the auction notice to hire the ICT is the way to detail the specific technology or communication network, not impairing or directing the hiring of a particular supplier.<sup>cdxviii</sup>

To enhance the capability of the members of the Public Administration, especially in the city level, it is interesting to have continuous training of the staff of public entities, as well as the development and distribution of reference guides for orientation of procurement procedures. These measures can help the Administration staff to identify the demand for products in a faster and easier way and to properly execute the demand of projects and bid notices.<sup>cdxix</sup>

#### Lack of Adequate Criteria to Select the Best Technical Solution

Another great challenge to the effective contracting of ICT solutions by the Public Administration is the absence of fast and flexible procedures for selection based on product quality.<sup>cdxx</sup> Conversely, the simplest bidding modalities are usually used for products widely available in the market and that can be acquired through the “lowest price” type of bidding. Additionally, the time taken to complete the bidding phases is sometimes incompatible with the development time of new technological solutions.<sup>cdxxi</sup>

In addition to legislation not flexible enough for the specificities of contracting technological solutions, the control bodies have reinforced a strict and formal bidding process. For some opportunities, the Court of Audit, due to lack of internal procedures capable of dealing with the specificity of hiring new technologies, has reinforced traditional bidding parameters.<sup>cdxxii</sup>

Moreover, there is no unanimity among the many Courts of Audit about bidding procedures, requirements and exemptions. This combination of factors fosters a scenario of uncertainty and discouragement in terms of public sector innovation. Managers begin to actively adopt bureaucratic procedures to avoid inspection and sanction by different control bodies.

#### Obstacles for the Auction Model: Terms of Reference and Lowest Price

Although the auction is a faster procedure, due to the inversion of the phases of qualification and proposal analysis, it requires the development of detailed Terms of Reference and only allows for contracting the lowest-priced offer.



In relation to the Terms, the base document of this bidding modality, it must include precise information on the product, supply strategy, estimated value based on market price, delivery schedule, among others (Article 9, Decree no. 5.450/2005). For ICT contracts, however, it is not always possible to present similar detail, since it often involves new products with no market equivalence. Even if such detail is available, the procedure may still be inadequate since the specificity required by the Terms of Reference may restrict suppliers and exclude different and innovative technologies from the range of potential solutions.<sup>cdxxiii\_cdxxiv</sup>

Another challenge of ICT contracts through auction is the lowest-price requirement,<sup>cdxxv</sup> as it limits the possibility of evaluating the technical quality of the ICT in relation to the specific needs of the contracting public body. This difficulty is more common in the acquisition of software, given its peculiarities and specifics, while contracting hardware through auction is less complicated.

In relation to the most-disseminated ICT, certain control bodies understand that their protocols, methods and performance and quality standards are established and known by the market. As a result, they have established that their acquisition would be better executed using the auction model.<sup>cdxxvi\_cdxxvii</sup>

#### Direct Contracting: Possibilities and Legal Uncertainty

One of the possible alternatives to acquire unique and innovative ICT not appropriate for the auction model is direct contract, due to exemption (Article 24) or unenforceability (Article 25, Law no. 8.666/1993) of bidding processes.

First, software and other technology solutions hired by the Public Power may be exempted from bidding processes even when there are other competing products and suppliers, whenever there is a possibility of hiring goods or services manufactured or provided by a body of the Public Administration (Article 24, III, Law 8.666/1993). This is the case of Serpro (Federal Data Processing Service), a public federal company that provides information technology services.

Law no. 5.615/1970, which regulates Serpro operations, exempts the Union from the bidding process for contracting information technology services that are considered strategic (Article 2). Likewise, Decree no. 8.135/2013 determines that (i) federal body data communications must use IT services provided by bodies or entities of the federal government itself; and (ii) bid exemptions are granted for contracting federal bodies or entities directed at protecting national security.

Second, ICT solutions may also be contracted directly, based on bid unenforceability when there is proof of the exclusivity of the product and the existence of only one supplier capable of providing the service. However, this possibility has caused uncertainties for public managers, with many decisions rendered by Courts of Audit removing the case's exceptionality. For example, in 2004 the Union Court of Audit rejected the direct contracting of Oracle software licenses by the National Petroleum Agency (ANP) due to the availability of other database software on the market.<sup>cdxxviii\_cdxxix</sup>

Finally, when direct contracting is chosen, based on exemption or impossibility of calls or bids, it is important to provide channels for suppliers to present their new products that may be of

interest to the Administration. This is relevant because managers tend to hire suppliers previously known to them.

#### Obstacles in Contracting Free Software: Efficiency versus Isonomy

“Free software” is a computer program created in a free and collaborative manner, allowing for its use, copying, changing or redistributing without permission from its original creator.<sup>cdxxx</sup> It is also essential for the free software to have a free source code, that is, it must be broadly known and not exclusively held by its owners.<sup>cdxxxi</sup>

In the chapter on urban mobility, we advocate that the adoption of free software by public bodies would ensure greater efficiency in public management,<sup>cdxxxii\_cdxxxiii</sup> since this may avoid the software contracting monopoly in governmental use, as well as the lock-in effect, due to technical difficulties in software migration and data transfers.

However, guidelines that indicate the Administration should privilege free software<sup>cdxxxiv</sup> create constitutional uncertainties and defy legal provisions on bids.<sup>cdxxxv</sup> The legality of previous and general selection of this type of software by the Public Power is questioned, since, according to a judicial update previously supported by the Federal Supreme Court,<sup>cdxxxvi</sup> this option does not comply with the principle of bidding isonomy, as it discriminates ex ante software suppliers under the legal bidding regime.<sup>cdxxxvii\_cdxxxviii</sup>

On the other hand, there is also advocating of the Administration’s option to choose free software, claiming it is compliant to the constitutional principle of efficiency<sup>cdxxxix</sup> - granting the Public Power the authority to exercise its purchasing power to inhibit creation and preservation of private monopolies -, which does not go against the principle of isonomy, since the Administration’s choice for free software is based on the very definition of bidding or its purpose and not on a technical capacity expected from the software.<sup>cdxl\_cdxli</sup>

Finally, as previously indicated, a recent Supreme Court decision considered constitutional the state law that establishes abstract preference for contracting free software, since the topic is of “regular” legal competency and does not lead to the exclusion of possible bidders from the universe of Public Power contracts.<sup>cdxlii</sup>

### 7.7. Smart Public Safety

IoT applications in the urban environment will also be used in the creation and improvement of existing systems for supporting public safety activities, through the use of new sensor technologies and high-definition connected cameras,<sup>cdxliii</sup> mechanisms that generate concerns regarding limits and necessary controls in order to prevent abuses by the State.<sup>cdxliv</sup>

These concerns are not new and reflect many of the already existing concerns regarding current surveillance camera systems. However, such concerns gain new meaning due to the expansion of the type and volume of data, as well as the development of technologies capable of automatically processing the data.<sup>cdxlv</sup>

It is important to emphasize that the State may implement surveillance mechanisms in IoT applications. As in the case of surveillance cameras currently available, these new monitoring actions by the Public Power are legally supported in the constitutional system, which states, in Article 144, that the State has the duty to guarantee Brazilian citizens security through the execution of efficient public security.<sup>cdxlv</sup> Constitutional jurisprudence itself includes the right to security as a "unavailable constitutional prerogative," which must be guaranteed through the implementation of public policies, which imposes on the State, therefore, the obligation to create objective conditions that allow effective access to such service.<sup>cdxlvii</sup>

Within this context, highlighted in Produto 8: Aprofundamento de Verticais - Cidade, the processing of personal data without prior and express consent is justified, on the condition that the processing of such data is strictly necessary and proportional to the purpose (guarantee of public safety), as well as carried out only by authorities in the public security system.

However, it is important to be aware that improvements in the capacities of the monitoring systems, in conjunction with the greater integration of these systems with a variety of sensors,<sup>cdxlviii</sup> challenges the limits of the constitutional prerogative of the state established in the mentioned Art. 144 and the above conditions. The progressive integration of new technologies into existing surveillance mechanisms has the potential to significantly achieve fundamental rights, such as the right to privacy and freedom of expression, which are also guaranteed by the Constitution.

In this way, the use of this new complex of technologies by the Administration in a responsible manner is recommended, with the application of checks and balances and considering notions of necessity and proportionality. Even if the police authority represents a power available to the Public Administration to condition and restrict the rights of individuals,<sup>cdxlix</sup> the measures should not be used beyond what is strictly necessary. Public security consists, according to the constitutional text, in a state action aimed at preserving or restoring public order, a circumstance in which individuals have the prerogative to enjoy all their rights,<sup>cdi</sup> including that of privacy.

From this perspective, public safety activities should be defined by prohibition of excess and by specific limitation with respect to the purpose to which the data are collected. It is fundamental to establish these limits as a way to safeguard individual liberties.<sup>cdii</sup>

In this way, the fundamental rights of citizens, including those concerning the inviolability of privacy and civil liberties, should be seen as a limit to the State's performance in the sphere of public security. Again, this does not mean prohibiting the collection or monitoring of data for public security purposes. However, it implies a prohibition of abuse. For example, use of the data for purposes other than those justifying its collection is prohibited. In addition, unused data should be discarded. There can be nothing arbitrary in the practice of data collection.

Also prohibited is the possibility of discrimination, for example, based on race and other socioeconomic characteristics. In addition, the data must be kept secure. Access to data for other purposes not directly related to public security will depend on a court order. Third party access to data or the transfer of the data to other entities should also be prohibited.

Evaluation of the effectiveness levels of the use of these new monitoring solutions is also necessary, since inefficiencies in such applications may create questions about the need for system

implementation, the training of the public agents involved, as well as the proportionality of the data treatment.

In Brazil, the effectiveness of the “Detecta” system<sup>cdlii</sup> has already called into question by the Court of Audit of the State of São Paulo (“TCE-SP”).<sup>cdliii</sup> The court questioned, among other aspects, the system’s ability to reduce the quantity of persons involved in the monitoring and to guarantee the confidentiality and security of the information. Generally speaking, it was understood that (i) there were failures in the planning for contracting of the service; (ii) the service is not often used by police units; (iii) there are errors in terms of security in accessing information.

Outside Brazil, the use of facial recognition techniques for the identification of suspects in the Boston terrorist attack also displayed problems. Images of two suspects were available in public databases, but the computers were unable to identify them.<sup>cdliv</sup>

As an example, it is worth mentioning how new systems with sound sensors in cameras and automated identification of individuals through facial recognition can be abusive in terms of guaranteeing fundamental rights such as privacy and freedom of expression.

A system of cameras with uninterrupted sound capture can generate recordings of the conversations of individuals in the streets in real time and in a historical series, which besides being an abusive intrusion in the intimacy of these individuals could also discourage public manifestations of individuals, resulting in a chilling effect.<sup>cdlv</sup> In the same way, a camera system with automated facial recognition could be used to monitor the movement and habits of individuals in general in real time and overtime, creating a precise database of each citizen preventively.

Therefore, while the use of surveillance cameras by public security organs is already an important element in the current strategy for assuring public security, safeguards and control mechanisms should be improved in order to avoid abusive surveillance practices with the modernization of systems and applications being used. In all cases, the benefits should always outweigh the burden. A surveillance system that shows little or no positive efficacy, while at the same time demonstrating negative effects (such as reducing fundamental rights) should be discontinued.

From this perspective of checks and balances, the European Forum for Urban Security<sup>cdlvi</sup> published the Charter for a Democratic Use of Video Surveillance.<sup>cdlvii</sup> The text presents general principles for the design and operation of video surveillance systems, including legality, necessity and proportionality. The Charter suggests that the use of surveillance solutions should first comply with local laws and international treaties dealing with privacy protection, monitoring of communications and use of personal data. Secondly, the public decision on the installation of such devices should be based on necessity. The document identifies necessity as the appropriate balance between, on the one hand, circumstances and urgency, and, on the other, the type of response - in this case, the use of surveillance equipment. Additionally, the action of the Administration must be proportional to the problem that it intends to resolve. In other words, there must be a level of appropriateness among the objectives of the activity and the means used to achieve them.

With a similar intent to ensure a balance between public security and individual rights, the recently published European Parliament's Directive 2016/680 focuses "on the protection of

individuals with regard to the processing of personal data by proper authorities for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and free movement of such data".<sup>cdlviii</sup> In considering item number 26 of this Directive, it is possible to identify the same targets for action within the legal limits, by means of necessary and proportionate measures.<sup>cdlix</sup>

In Brazil, it is important that this agenda also progress. With so many new solutions focused on public security that involve collection of personal data, good practices for treatment of this information is essential to avoid abuses by public security agencies or others. As already indicated by other documents referenced, essential measures will include adoption of a specific law for the protection of personal data and the creation or designation of a personal data protection authority.<sup>cdlx</sup>

In addition to this initiative, progress must be made in the development of a framework of good practices by the Public Power. Possible initiatives include the adoption of a Data Protection Impact Assessment (DPIA), to identify privacy issues and decide which procedures to follow to ensure that risks are managed. Another interesting possibility is the design of a code of conduct that establishes guidelines on how public safety agencies should implement and operate current and future monitoring systems for cameras and sensors. Among the questions that may be addressed, we highlight the following:

- a) Establishment of the functionality, and their respective parameters, to be adopted as best practices in monitoring by cameras and sensors in public safety activities;
- b) Establishment of clear information and communication tools for camera and sensor monitoring to the public, except for authorized secret monitoring;<sup>cdlxi</sup>
- c) Definition of parameters of the timeframe for data storage, for each type of monitoring. In some cases, it may not even be necessary to retain data, as with sensors for capturing audio in public places;
- d) Definition of policies for data sharing among public security agencies, prohibiting sharing for reasons other than public security.

## 8 Health

The objective in this portion is to identify the regulatory aspects related to the Internet of Things (IoT) in the healthcare area, and to map possible regulatory barriers that impact the development of this technology in the sector, especially in relation to the following prioritized applications<sup>cdlxii</sup>: i) remote monitoring of the conditions of patients with diabetes; (ii) location of assets within health units; (iii) support for a diagnosis of sepsis; (iv) decentralized diagnosis; and (v) identification and control of epidemics.

It is important to clarify that this regulatory analysis will not focus on each specific application, since it is first important to outline a general diagnosis of sector legislation. Then, if necessary, an analysis those items specifically related to the selected applications will follow, if needed.

To meet the proposed objective, the methodology used to develop the regulatory diagnostic of IoT in the health environment involved (i) the mapping of standards that impact the sector, especially the norms and guidelines established by the Ministry of Health (MS), National Health Surveillance Agency (ANVISA) and the Federal Council of Medicine (CFM); (ii) interviews with ANVISA technicians; and (iii) contributions from health sector agents who participated in workshops conducted by BNDES and the Ministry of Science, Technology, Innovation and Communications.

## 8.1 Regulation of the National Health Surveillance Agency – ANVISA

As explained in the Technological Roadmap (Version 2.0),<sup>cdlxiii</sup> the common elements of IoT are: (i) receiving of digital data from sensors and/or going to actuators; (ii) connection to a network outside the object itself; and (iii) the ability to automatically process data.

Following this definition, the next step was to identify health sector legislation with potential impact on applications involving the technology described, especially for health products and services of interest to the health surveillance system.

In this sense, in analyzing the sectoral legislation, it was determined that Law no. 6.360, September 23, 1976 ("Law no. 6.360/76"), states that no product of interest to the field of healthcare, whether domestic or imported, may be industrialized or placed for sale or consumption in the Brazilian market prior to registration at the Brazilian Ministry of Health.<sup>cdlxiv</sup> Even in the hypothesis of an exception to the registro registration, the product still requires a cadastro registration (Paragraph 1 of Article 25 of this law).<sup>cdlxv</sup>

It is important to clarify that this law was regulated by Decree No. 79.094 of January 5, 1977 ("Decree No. 79.094/77"), subsequently revoked by Decree No. 8.077, of August 14, 2013 ("Decree No. 8.077/13" ), which granted ANVISA the jurisdiction to register products subject to the health surveillance regime.

Law no. 9.782 of January 26, 1999 ("Law no. 9.782/99") in turn created the Agency and instituted the National Health Surveillance System, granting to ANVISA the jurisdiction to regularize, control and inspect products<sup>cdlxvi</sup> and services that present a risk to public health.<sup>cdlxvii</sup>

This same legal item offers the list of products and services subject to ANVISA sanitary inspection. Among the products listed in Art. 8, paragraph 1 of Law 9.782/99, include: (i) medications for human use, its active substances and other inputs, processes and technologies; (ii) kits, reagents and supplies intended for diagnosis; (iii) medical and hospital equipment, dental and hemotherapeutic equipment and laboratory and imaging diagnosis; (vi) radioisotopes for in vivo diagnostic use and radiopharmaceuticals and radioactive products used in diagnosis and therapy; (vii) any products involving the possibility of health risk, obtained by genetic engineering, by another procedure or even subjected to radiation sources.

Healthcare services, in turn, are defined in the following paragraph on the above-mentioned device as those for outpatient care, whether routine or emergency, those performed in an inpatient setting, diagnostic and therapeutic support services, and those involving the incorporation of new

technologies. Given that IoT technology is developed through devices, however much they may have an impact on health services, there will be no rules that regulate health services in the IoT.

Finally, it is important to emphasize that the concept of health surveillance is related to a set of actions capable of 1) eliminating, reducing or preventing health risks and intervening in health problems caused by the environment 2) controlling production and circulation of goods and the provision of services of health interest, which may include: (i) controlling consumer goods that directly or indirectly relate to health, including all steps and processes, from production to consumption; and (ii) controlling the offering of service directly or indirectly related to health.<sup>cdlxviii</sup>

With this initial description of the sector's legislation provided and the central role of ANVISA is understood as the federal agency responsible for sanitary surveillance, an analysis of the agency's regulatory standards follows.

## 8.2 Health Products

### a) Characterization

As explained above, health products can only be industrialized, placed for sale or delivered for consumption in the Brazilian market after being registered with ANVISA, either through the registro or cadastro registration process.

Resolution no. 185, of 2001 ("RDC 185/01") defined a health product as "equipment, apparatus, material, article or system of medical, dental or laboratory use or application intended for prevention, diagnosis, treatment, rehabilitation or contraception and does not use pharmacological, immunological or metabolic means to perform its main function in humans, but may be assisted in its function by these means".

From the above definition, the determining aspect of a "health product" is related to its therapeutic or diagnostic purpose. This definition creates uncertainty when the product involves some technological solution, which is already the case with using software in healthcare, which can be used as a parameter for IoT applications.

In an attempt to clarify the rules on software for healthcare, Technical Note no. 04/2012/GQUIP/GGTPS/ANVISA was published, which sought to shed light on determination of registro or cadastro for software.

IoT applications will always contain some software device in one of the links of its value chain, and since there is no specific rule related to the products operated with IoT, it is important to understand the conclusions of this guidance. This is because they could serve in the analysis of the IoT solutions framework for health products.

Under the scope of the Technical Note, ANVISA concluded that software can fall into three categories:

	Definition	ANVISA Actuation	Example
Software product for healthcare	Does not need hardware classified as a product for health in order to be executed	Can only be industrialized, placed for sale or delivered for consumption in the market after cadastro or registro registration with ANVISA.	Software used for medical data processing; for surgical positioning and to diagnose a disease, such as Match It! DNA Software and the ZSCAN Image Capture and Reporting System.
Software part of accessory for a healthcare product	Is an integral part of hardware, requiring it to function	It must be registered in conjunction with the hardware (except in certain cases) Technical Note 04/2012 <sup>cdlxix</sup> )	Software that controls the functions of a medical device or transfers information about equipment, doctors such as Picture Archiving and Communication System (PACS)
Software not for healthcare	They are intended for purposes other than prevention, diagnosis, treatment, rehabilitation or contraception of human beings.	Not subject to registro or cadastro at ANVISA.	Apps for mobile devices, specifically designed for sports and leisure, such as Apple Watch or Fit Bit

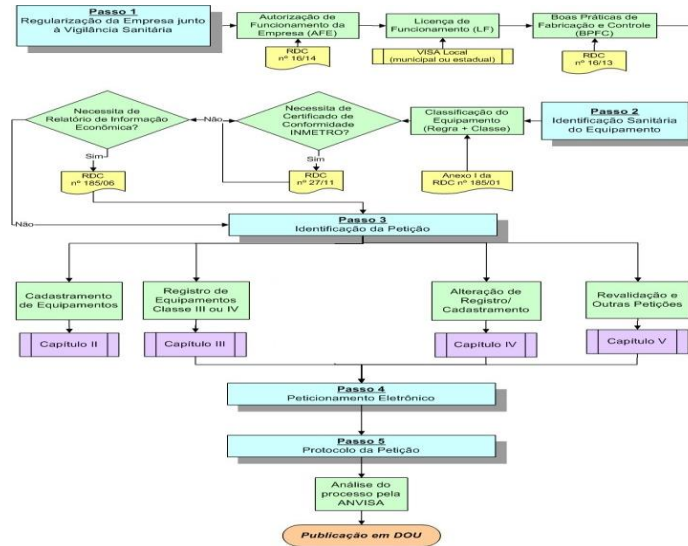
Based on the above information, it can be concluded that when equipment that involves IoT technology has a therapeutic or diagnostic purpose, it will be framed as a health product and is therefore subject to sanitary surveillance.

b) Registration Process (registro and cadastro)



An understanding of the types of registration processes with ANVISA is relevant for the identification of possible barriers for development of IoT in the health area.

The procedure for the registro registration is overseen by RDC 185/01 and according to Decree no. 8077, of 2014, should be granted in 90 days.<sup>cdlxx</sup> The procedure for the cadastro registration is simpler and is regulated by RDC no. 40 of 2015 ("RDC 40/2015"). The image below, taken from the ANVISA Manual for Regularization of Medical Equipment, shows the flowchart for the entire registro and cadastro request process at ANVISA<sup>cdlxxi</sup>.



The flow chart above shows that previous steps that must be carefully followed when requesting registro or cadastro with ANVISA, as insufficient required technical documentation may lead to a summary rejection of the petition,<sup>cdlxxii</sup> which will delay the process.

Therefore, the first step in requesting the *registro* or *cadasto* of medical equipment at ANVISA is the regularization of the company by obtaining (i) the Authorization for Operation of the Company (known as the "AFE"), (ii) of the Local Operation License (known as "LF") and (iii) of the Good Manufacturing and Control (known as "CBPF") Certificate.

The Authorization for Operation must be obtained pursuant to RDC no. 16, of April 1, 2014, and only companies legally constituted in Brazil can petition this authorization from ANVISA.

It is important to keep in mind that according to this manual, a foreign company with an interest in marketing its products in the Brazilian market must have a commercial agreement with a company in Brazil. The Brazilian company need not be a subsidiary or affiliate of the foreign company, in which case the Brazilian company may only be an importer, assuming the technical and legal responsibility of the foreign company in Brazilian territory.

In addition to the Authorization for Operation of the Company, a Local Operation License must be issued by the local health surveillance agency, whether state or municipal. Following this, the company must meet the requirements of Good Manufacturing and Control Practices, which is an obligation of any company intending to manufacture, import or market medical products, as provided by Decree No. 8.077, of August 14, 2013.

After this proof, a certificate of Good Manufacturing and Control Practices is issued, the presentation of which is obligatory for the registration of Class III and IV products. For Classes I and II products, subject to recording, presentation is not necessary, however, the requirements as established in Resolution 16/2013 must be met.

The technological evolution within IoT technology may require updating of Good Manufacturing and Control Practices. However, there are no indications that the current requirements represent a barrier to current applications. Following this step is sanitary identification of the equipment; identification of equipment risk class (from Class I to IV) is required.

In addition to risk classification, the product must be classified by rules, aligned with indication and purpose of the equipment. These are: (i) non-invasive products - rules 1 to 4; (ii) invasive products - rules 5 to 8; (iii) active products - rules 9 to 12; and (iv) special rules - rules 13 to 18. Such classification rules can be found in Annex II of the Technical Regulation approved through RDC 185/01.

A reading of the Resolution shows that there exist several rules which present complex classification criteria, possibly making it difficult for agents to classify the product, which consequently increases processing time.

Following this, it must be determined if a product is subject to cadastro or registro registration.<sup>cdlxxiii</sup> Cadastro has its legal foundation in Paragraph 1, Article 25 of Law no. 6.360/76 and is governed by RDC no. 40, of August 26, 2015<sup>cdlxxiv</sup>, applied to healthcare products classified in risk class I or II, with the exception of products for in vitro fertilization.

The procedure for the cadastro request from ANVISA is found in Article 4 of RDC no. 40/2015, among them (i) request form for registry of product information; (ii) proof of payment of sanitary surveillance inspection fee; (iii) certified copy of the certificate of compliance, applicable to medical products with compulsory certification; (iv) apostilled statement accompanied by a sworn translation for imported medical products.

Detailed presentation of product data is required to complete the form. Given the need for such highly detailed information, the involved parties may have questions, which can be addressed in the Manual for Regularization of Medical Equipment at ANVISA.

Software registration requires filling out of the proper form. At this point, there may emerge questions about the need to fill out the form to register IoT products since, generally speaking, applications with this technology will have a software device at some point in the chain.

Details on the information may also be found in the above-mentioned Manual and involve information such as software architecture, compatibility (interoperability and communication) with other medical products and infrastructure requirements, among others

The manufacturer or importer of the product should maintain an updated technical dossier,<sup>cdlxxv</sup> to allow inspection by the National Health Surveillance System. The dossier should describe the elements that comprise the product, with the indication of characteristics, purpose, use, content, special care, potential risks, production process and additional product information.

Finally, it is not necessary to revalidate the cadastro and its maintenance is linked to compliance with the requirements of Good Manufacturing Practices.

Class III and IV equipment, on the other hand, are subject to registro, and a greater number of documents, provided for in RDC 185/2001, must be submitted to ANVISA, compared with cadastro. They are: (i) manufacturer or importer's completed form on medical product; (ii) proof of payment of the sanitary surveillance fee; (iii) company data - copy of authorization to function document; (iv) label; (v) unchangeable tag; (vi) instructions for use; (vii) technical book; (viii) proof of compliance with the requirements established in technical regulations; (ix) Certificate of Good Manufacturing Practices and Control.

For imported products, the following must still be presented: (i) a letter of authorization of representation in Brazil issued by the manufacturer abroad; and (ii) Free Trade Certificate.

Software registration also requires specific requirements, which can be summarized as follows: (i) software architecture; (ii) hardware architecture; (iii) minimum and recommended technical requirements; (iv) platform; (v) compatibility; (vi) safety features; (vii) infrastructure requirements; (viii) verification (list of tests performed, their failure or success criteria and the percentage of approval obtained in them).

It should also be noted that the Technical Book referred to as one of the documents that must be presented for registration should describe the efficacy and safety of the medical product, the requirements of which are indicated in Resolution No. 56 of 2001 (RDC 56/2001").

Such requirements guide the manufacturer regarding possible risks, which need to be controlled, and it is the sole responsibility of the manufacturer to analyze, evaluate and control the risks associated with his product.

These will be checked by the sanitary surveillance authority when inspecting Good Manufacturing Practices, registering with ANVISA or during sanitary inspection of products. If the description in the Technical Book does not prove the efficacy and safety of the product, ANVISA will request clinical research, specifically research using humans, to verify the performance and safety and effectiveness of the product, in accordance with the Resolution No. 10, 2015 ("RDC 10/2015").

Finally, in terms of validity period, the timeframe is 10 years, and may be revalidated for an equal period of time.<sup>cdlxxvi</sup> It is important to note that the equipment is authorized to be marketed only after the registro registration or the cadastro registration. The product marketed must

necessarily correspond to what has been authorized by ANVISA and any changes in such equipment must be made by petition to the agency.

#### Need for Regulatory Updates

As described in the regulation that governs ANVISA's framework for products, applications analyzed in this Book will likely be subject to cadastro registration or registro registration, depending on the level of risk of the application.

However, considering the many possible applications for IoT and constantly and rapidly evolving technologies, a concern is regulation and its ability to keep pace with advances in technology. An example of this challenge is combined products, such as drug-device combination products<sup>cdlxxxvii</sup> which are therapeutic and diagnostic products that combine medications with devices.

Given that the product definition in RDC 185 excludes pharmacological products from that classification, the health status of this type of product is called into question, as well as how the Agency will regulate other complex products emerging from technological advance.

In addition to the need to constantly update the standards that regulate a developing sector, another challenge is the difficulty of sector regulation to translate or address public health risks related to software as medical devices or IoT solutions specifically, and ensuring the appropriate balance between patient/consumer protection and public health promotion by encouraging innovation.

The International Medical Device Regulators Forum ("IMDRF"), an international forum of regulators from several countries, regularly updates the rules that regulate software as a medical device, in order to ensure regulatory convergence among the regulatory bodies of the various countries that comprise it.

Regarding this aspect, ANVISA's General Management of Technology for Health Products suggested both in interviews with technicians from the area as well as at the International Seminar on Medical Devices 2017 that the Agency's 2018/2019 regulatory agenda will provide for development of a Specific Resolution for regulation and control of software as a medical device.<sup>cdlxxxviii</sup>

The updating of this rule will consider the IMDRF guidelines. These would include: (i) N10, which establishes the definitions and terminologies applied to software as a medical device;<sup>cdlxxxix</sup> (ii) N12 which provides information on risk classification,<sup>cdlxxx</sup> (iii) N23, which discusses a quality management system,<sup>cdlxxxii</sup> and (iv) the N41R3, which regulates clinical evaluation of software.<sup>cdlxxxiii</sup> Beyond this, the Agency also evaluates the internalization of the U.S Food & Drug Administration – FDA-Guide for Cybersecurity,<sup>cdlxxxiii</sup> which will be further discussed in the chapter on data protection.

Given this, the subject of software as a health product will likely be updated soon, which will alter the scenario explained in the previous items. Such an update, however, seems to be in keeping with the industry's most advanced practices and international standards.

### 8.3 Regulation of Councils of Medicine

The role of the Federal Council and the Regional Councils of Medicine, serving as an authority, is supervision of medical ethics.<sup>cdlxxxiv</sup>

Although the Council's standards do not create obstacles for development of IoT solutions in the health area, they should always be followed by physicians in the exercise of their profession, regardless of the technological environment used in their work.

The Federal Council of Medicine, seeking to adapt the practice of the medical profession to the technological advances in the health area, has already regulated the use of digital medical records<sup>cdlxxxv</sup> (Resolution no. 1.821/07) and telemedicine<sup>cdlxxxvi</sup> (Resolution no. 1.643/02).

In regards to digital medical records, Resolution No. 1.821/07 deals with the digital storage and handling of patients' medical records. In some respects, it equates the digital file with the physical, showing the need to maintain professional confidentiality and privacy of the individual, according to the Code of Medical Ethics. Following this, the resolution raises some specific rules for the digitization of medical records, such as the parameters that specialized electronic management systems should have, including guarantees of security.

It should be noted that the Resolution also provides for the signing of an agreement between the Federal Council of Medicine and the Brazilian Society of Health Informatics to issue a quality seal for computerized systems. This, combined with the recognition of technology's positive impacts on patient care, demonstrates the Federal Council of Medicine's concern in absorbing and regulating technological advances in the healthcare area, and may regulate the impact of IoT technologies in the future.

In terms of telemedicine, Resolution no. 1.643/02 seeks to address "the practice of Medicine through the use of interactive audiovisual communication and data methodologies, with the objective of healthcare services, education and research."

The Resolution allows doctors to practice telemedicine, aligning this practice more closely with regular medical practice. In addition, it establishes that telemedicine must also be based on confidentiality, privacy and professional secrecy, which must be guaranteed by the technological infrastructure that is used to provide such a service.

As the Resolution is justified by emergence of new technologies and its comprehensive definition focuses on "interactive audiovisual and data communication methodologies", such a standard can apply to future IoT equipment and technologies in healthcare.

Given this, it is possible that technological advancement from IoT could also result in innovations that demand the updating of these council norms. It is important that these standards adequately protect health and medical interests, stimulating technological advances.

### 8.4 The Debate on Privacy

#### a. Privacy and Health

IT applications in the health area may (or may not) involve the collection of personal data. A case of personal data usage would be, for example, remote monitoring of patients with diabetes and in the diagnosis of sepsis.

As we previously demonstrated in the section on technological analysis of applications, the guarantee of confidentiality and data privacy is critical for adequate development of IoT applications in the healthcare area.

Therefore, privacy and personal data deserves special attention due to the need to safeguard the privacy of individuals while also enabling the State, research institutes and private health organizations to access relevant data for development of public policies or technological advances in the sector.

Given that the utilization of IoT devices in the health area will increase the data collection capacity of citizen information, we will contextualize and analyze the rules regarding privacy and data protection in the healthcare area.

As explained in Product 3,<sup>cdlxxxvii</sup> there is still no general data protection law in Brazil. It is important to emphasize that the absence of this general standard impacts IoT, especially in the healthcare area, where data collected is particularly sensitive and requires special attention.

Despite the lack of a general data production law, there are currently three bills before Congress on this topic. Among them are bills no. 4.060/2012,<sup>cdlxxxviii</sup> no. 330/2013,<sup>cdlxxxix</sup> and no. 5.276/2016,<sup>cdxc</sup> which, among other aspects, distinguish personal data from sensitive personal data.

It is important to note that increasing personal data protection in healthcare is included in these bills. While in Bill 4.060/2012 only genetic data is considered sensitive, with no mention of health data in general, the other bills portray health data as sensitive data.

In the case of Bill no. 330/2013, Article 5 establishes requirements for the collection, storage, processing, transmission, use, provision or disclosure of sensitive data.

Among these requirements are the express, specific and unequivocal consent of the data subject, as well as the existence of relevant public interest, which could be for purposes of preventive medicine, diagnosis or medical treatment, and management of healthcare services.

The abovementioned provision further determines that treatment of such sensitive data for relevant public interest may only be conducted by direct public administration bodies, public legal entities or private law legal entities in the exercise of medicine or healthcare protection.

Finally, Bill no. 5.276/2016 is even more restrictive in the definition of sensitive data, including not only health data but also biometric data. It also provides for the need for consent in processing of sensitive data, gives the data subject the right make data anonymous, and blocks or deletes unnecessary or excessive data. However, in the absence of a specific law on the protection of personal data, disparate rules apply, in particular the Federal Constitution, the Internet Framework and the Consumer Defense Code, as explained in detail in Product 3.

Another relevant aspect is cybersecurity. Considering that medical devices are subject to attacks, especially when connected to the Internet, strategies must be created to mitigate these risks.

As already explained at the International Medical Devices Seminar 2017,<sup>cdxci</sup> the agency, in referring to the ANVISA regulation, Cybersecurity Guidance from the U.S Food & Drug Administration (FDA)<sup>cdxcii</sup> said it would be incorporated into the 2018/2019 regulatory agenda. Therefore, among the main FDA guidelines to mitigate the cybersecurity threat is the need for medical device manufacturers and health facilities to adopt safeguarding measures. In this regard, manufacturers must be vigilant in identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. Hospitals and health facilities are responsible for evaluating the safety of their network and protecting their hospital systems.<sup>cdxciii</sup>

Following this brief introduction, the following analyzes health sector personal data and privacy protection issues that would most impact IoT.

#### b. Collection of Personal Data

For applications that will involve data collection, the first relevant aspect involves the need to obtain valid consent for this collection.

When an individual agrees to a service in the public or private health sector that implies the use of personal information, the contracting of this service will imply consenting to the collection and use of such data for the specific purpose of that service. The data will, in turn, be protected by medical confidentiality.

The sensitive issue relates to cases in which such data can be used for purposes other than treatment. In this hypothesis, the express consent of the individual is fundamental, as is providing information on the purpose of the data.

Therefore, when the app is operated through devices that interface with the patient (and also through smartphones as is the case of the application developed for diabetes monitoring) there must be a privacy policy with express consent for personal data collection, use, storage and processing, under the terms of Article 7, item IX, of Law no. 12.965, of April 23, 2014<sup>cdxciv</sup> ("Internet Framework").

Yet, as suggested in the Smart Cities chapter, it is important to plan data collection based on the concept of "privacy by design"<sup>cdxcv</sup> meaning that the very design of the product or service that will collect data must consider privacy protection from its inception.

When IoT solutions operate restrictively in health units and must be operated by a health professional, as is the case of the application described for decentralized diagnosis, the patient must be capable of agreeing to the data collection policy of this application.

Additionally, it should be noted that, given the sensitivity of personal data in the health sector, confidentiality must be maintained. In this sense, standards embedded within the health system itself establish the duty to maintain confidentiality of users' personal information in Ordinance no. 1.820 of 2009 of the Ministry of Health. This standard provides for the rights and

duties of patients and advocates for the confidentiality of any and all personal information during appointments, diagnostics, preventive, surgical, therapeutic and hospitalization procedures.<sup>cdxcvi</sup>

Therefore, although there is no legal manifestation on the collection and use of personal data, the Ministry of Health has already shown a clear need to maintain confidentiality and formalize health service user consent for data collection.

c. Processing of personal data

Regarding the processing of personal data, as already discussed in the same topic related to the "Smart Cities" environment, one of the emerging problems is the use of data for purposes other than the one consented to by the individual.

As explained, the express consent of the user is essential for the collection of personal data for purposes other than that of the contracted health service.

Beyond that, the use of data must have the same purpose as reported to the citizen when obtaining consent. If data is used for purposes other than the one reported, then there must be new consent or anonymization, aggregation and use of techniques such as differential privacy, always in a manner that is technically safe and prevents revealing the information.

In the health sector, it is worth noting that, within the scope of public health, there exist cases in which information must be obligatorily provided to the public power by legal duty, without any need for obtaining consent.

For example, Law no. 6.259 of 1975 mandates compulsory notification of diseases for epidemiological investigation by sanitary authorities. This law stipulates that the notification be confidential, with anonymization of the patient's data, except if there is exceptionally high risk to the community.<sup>cdxcvii</sup> In this case, although consent is not required, the purpose of the use of data must be respected.

Finally, the use of data by the Public Power must respect all principles of legality and public interest. This means that the finalities for which the State uses citizens' data must be provided for by law and constitute a purpose that attends to the public interest.

d. Storage of Personal Data

Security of information processed by technological devices as well as data collected and stored in the cloud is a common concern. This concern shows a need to adopt privacy and information security measures for personal data storage.

Therefore, to guarantee greater security in data storage, the tools should be used for the aggregation and anonymization of information collected by IoT devices. Furthermore, it is worth noting that in 2017, the Ministry of Health reinforced its data protection and information security policy through the publication of Ordinance 271, of 27 January 2017,<sup>cdxcviii</sup> following the recommendation of the Court of Audit of the Union.<sup>cdxcix</sup>



The purpose of this policy is to promote greater security in the processing, storage and communication of data in the computer systems of the Unified Health System (known as “SUS”) and in the network of the Ministry of Health. Therefore, this data protection policy may impact the security of information in IoT applications in the public health network.

The policy should be based on the principle of privacy, which determines that information that harms the intimacy, integrity and honor of citizens may not be disclosed.

The standard also establishes a series of guidelines for data and information protection, with emphasis on the responsibilities and duties of public agents.<sup>d</sup> Among these guidelines is the regulation of ownership and handling of the information which, among other rules, establishes the following:

- (i) Every item of information that is created, handled, stored, transported, discarded or stored by the Ministry of Health is of its responsibility and should be properly classified and protected regarding aspects of confidentiality, integrity, authenticity and availability, in explicit or implicit ways, according to Decree no. 7.845 of November 14, 2012, which provides for procedures for security accreditation and treatment of information classified under any degree of confidentiality; and
- (ii) the information produced, stored and transported in electronic means will use encryption compatible with degree of confidentiality, especially user authentication information in the applications.

This Order advanced by establishing mechanisms to control information through monitoring and auditing,<sup>di</sup> as well as rules on cloud computing that assure the availability, integrity, confidentiality and authenticity of information hosted in the cloud.<sup>dii</sup>

e. Sharing of personal data

The sharing of collected data is an extremely relevant topic that faces challenges, such as the need for privacy protection, the guarantee of interoperability and the adequate exchange of information among information systems at health institutions.

Sharing of data in the health sector could be required for many reasons, such as the need for information sharing among public or private healthcare units for the treatment of a specific patient, for research, or for commercial purposes.

In any case, as a rule, it is imperative to obtain voluntary, express and informed consent from citizens.

Additionally, when the data sharing occurs for purposes other than treating the data requester, as for research or commercial purposes, it is necessary that the data is anonymized in a definite and safe way, as well as aggregated and subjected to techniques like differential privacy.

Yet, whenever the data is accessed by third parties, even if anonymized, it must be protected by high security standards and not shared or used in any process of de-anonymization of data.

Other than that, another barrier found in sharing data is the interoperability and exchange of information in the health sector.

In meetings of the Health IoT Work Group, conducted by BNDES and the Ministry of Science, Technology, Innovation and Communications with representatives of the public and private sectors, this subject was brought up as a barrier to the adequate development of IoT.

The incentive for interoperability in the sector may occur through the regulation of criteria by the public power, or by autoregulation of agents of the sector.

Currently, Ordinance no. 2.073 of August 31, 2011, of the Ministry of Health, regulates the use of standards of interoperability and information of health for information systems within the Unified Health System (SUS) at Municipal, District, State and Federal levels, and for private systems in the supplementary health sector.

Among the objectives of this policy is use of a health information architecture with concepts that allow the sharing of health information and the cooperation of all health professionals, establishments and others involved in healthcare provided to users of the SUS, in a safe, respectful environment with the right to privacy.

Given the relevance of interoperability of data in the health sector, it is important that these norms and practices be continually improved, and that privacy is always assured through respect for consent and purpose for which data sharing has been authorized.

f. Access to Collected Data

Regarding access to collected data, all public organs that integrate direct administration, as well as municipalities, foundations, public companies and mixed-economy companies at all levels of the federation, are subject to Law no. 12.527 of November 18, 2011, ("Law of Access to Information").

In this sense, the access to information by public organs and health entities should be governed by this law and by Decree no. 7.724 of May 16, 2012. Beyond this, Ordinance no. 1.583 of July 19, 2012, of the Ministry of Health, provides information on execution of the Law of Access to Information in the scope of this Ministry and related entities.

As previously explained, the Law stipulates that personal information must be treated in a transparent way and with respect for the intimacy, private life, honor and image of people, as well as for individual freedoms and guarantees.

Access to such information will be restricted to the subject of the information and to legally authorized public agents, regardless of classification of confidentiality and for the maximum time frame of 100 (one hundred) years counting from the date that the information was produced.

The access to this type of information by third parties, in turn, may only occur if legally provided for or with the express consent of the individual.

However, such consent may occur when the information is for (i) prevention and medical diagnosis, when the person is physically or legally unable, and exclusive use for medical treatment; (ii) compiling statistics or scientific research of evident public or general interest, provided for by law, concealing the identity of the person to which the information belongs; (iii) compliance with a court decision; (iv) the defense of human rights of third parties; or (v) the protection of the general public and ruling interest.

Additionally, access to personal information by third parties will require signing of a term of responsibility, which will state the purpose and destination that justify the authorization, as well as the obligations of the requesting party.

The Ordinance also states that use of personal information by third parties is only for the purpose and destination that justify the authorization of access, prohibiting its use in various ways.

It is worth noting that this norm also applies to private non-profits that receive public resources.

Regarding the other private institutions, the standards provided for by the Law of Access to Information should also guide access to personal information within the scope of private health institutions. Only the individual or his or her legally authorized public agents can access personal health data, with access to data by third parties only permitted when expressly authorized by that individual.

## 9 Rural Environment

The rural environment has many characteristics and issues that demand a particular analysis in comparison to the other prioritized environments.

Among the analyzed regulatory concerns, three topics stand out: a) the availability of a connectivity infrastructure and its related regulatory aspects; b) regulation on the use of drones in rural IoT applications; and c) ownership and protection of data in the rural environment. The issues related to telecommunications were addressed in item 2.1 of this document, while the remaining issues will be presented below.

### 9.1. Use of Remotely Piloted Aircraft Systems (“RPAS”) in IoT Applications

Some rural IoT applications may benefit from the use of Remotely Piloted Aircraft Systems (RPAS), also known as drones.

#### a) Regulatory Framework

These aircraft have their general use regulated by three distinct entities in the country: a) the National Telecommunications Agency (ANATEL), b) the National Civil Aviation Agency (ANAC) and c) the Airspace Control Department (DECEA). For the safe and legal use of drones, it is therefore necessary to follow the regulations of these three entities.

The first regulatory element to be observed is related to ANATEL. The competency of ANATEL regarding drones is related to the need for approval of the connectivity modules present in these aircraft: for their operation, drones need radiofrequency transmitters in their remote piloting stations, as well as, in some cases, in the aircraft itself for the transmission of images.<sup>diii</sup> This approval aims to avoid the connectivity modules of irregular drones from interfering in other telecommunication services.

The operation must also comply with ANAC regulations. Within its competency of regulating and inspecting civil aviation activities, ANAC published the Brazilian Special Civil Aviation Regulation no. 94 (“RBAC-E no. 94”)<sup>dii</sup> establishing rules for civil RPAS operations. Among its provisions, the safe use of drones demands maximum take-off weight of 250 grams, in addition to: a) the operation within a minimum distance of 30 horizontal meters from buildings and facilities,<sup>dvi</sup> and from persons not involved in the operation;<sup>dvi-dvii</sup> b) the hiring of an insurance plan that covers damages to third parties;<sup>dviii</sup> c) the non-use of autonomous drones;<sup>dix</sup> and d) that each drone pilot operates only one equipment at a time.

Once the regulatory requirements of ANATEL and ANAC have been met, the drone operator must then comply with the requirements of DECEA<sup>dx</sup> to be able to use the airspace.

DECEA regulations are very important to ensure safe use of airspace, enabling the coordination of its use by different agents (commercial aircraft, military aircraft, ultralight aircraft, helicopters, drones, among others).<sup>dxi</sup> In order to establish the fundamentals for this use by drone operators, DECEA published the Aeronautic Command Instruction 100-40 (“ICA 100-40”).<sup>dxii</sup>

In addition, it is important that IoT development in the rural environment comply with legal or regulatory provisions that are specifically related to the activities being performed with the use of drones. As an example, we have aerobatics<sup>dxiii</sup> and the application of pesticides.<sup>dxiv</sup>

Finally, it is important to point out that, other than these specific regulations, the operation of drones is also subject to the application of legislation regarding civil, administrative and criminal responsibilities.<sup>dxv</sup>

#### a) Discussions in the rural environment

During the interviews and workshops held, many participants indicated that the current regulations for use of drones impedes development of IoT applications, especially regarding costs for compliance. According to these participants, the regulation focuses on the urban use of drones, which limits the opportunities and possibilities of the scaled use of drones in the rural environment, with very different conditions that demand less technical requirements. Among the given examples are the impossibility of autonomous operations, the redundancy of systems and the need for observers in the use of drones in some cases.

The new regulation established by ANAC in its RBAC-E no. 94, has provided legal certainty to the sector that operates drones, providing clear requirements for the use of these devices in different categories. Other than that, the dialogue and higher integration among the systems of the three regulatory entities have reduced complexity for compliance with legal obligations related to drone operations.

One of the concerns regarding autonomous operations was even clarified by ANAC, as the prohibition of autonomous operations does not imply a complete prohibition of entirely automated flights, which are allowed provided that the remote pilot can intervene at any time.<sup>dxvi</sup> Therefore, the requirement is for the activity to be monitored.

However, since these regulations are subject to change alongside advances in technology – in case there are technological improvements to technically guarantee that the precautions required by the regulation are no longer justifiable in the rural environment –, advocating for a more flexible regulatory regime for the rural environment seems possible.

Therefore, in order to develop the regulatory framework regarding drones in the rural environment, it is important to coordinate with the private sector and the Brazilian Precision Agriculture Committee (known as “CBAP”), within each competency, with further technical analysis of the latest in drone technology in the rural environment, in order to identify safe possibilities for easing the current regulatory framework, when applicable.

This material could serve as a support for dialoguing with regulating entities, seeking to change proposals for current regulations. Here it is worth mentioning that the very framework provided by ANAC for drone regulation (special regulation) indicates the Agency’s own intention to improve the related regulatory framework as experiences and technologies develop.<sup>dxvii</sup>

## 9.2. Data and Database Protection and Ownership

Another point highlighted in the analysis of the consortium and in market information is the concern regarding the protection and ownership of data and databases generated through IoT technologies in the rural environment, as well as possible personal data which would be involved in IoT solutions. This debate is complex, and there are deep divergences among large groups involved – with agricultural producers one on side and agricultural input/technology companies on the other.

To begin with, it is important to present the divergences on the subject.

Seeking greater protection for agricultural producers and cattle breeders in the new data economy, the Brazilian Agriculture and Livestock Confederation (known as “CNA”) has raised concerns about the privacy and security of rural data (including personal data). The focus of the entity is on strategic rural data, including “basic data”, from “harvester” sensors for example (that is, the possibility of obtaining real-time data on crops and harvest).

Among the concerns already presented by Confederation is the possibility of rural data being used to influence the commodities market,<sup>dxviii</sup> plus the possible inadvertent sharing of this data, especially in the current market reality.<sup>dxix</sup>

To deal with this scenario, the Confederation has advocated for greater protection of rural data, presenting as an example the self-regulation document negotiated by the American Farm Bureau Federation (AFBF), titled “Privacy and Security Principles for Farm Data”,<sup>dxix</sup> signed by 39 technology service provider companies, on the topic of precision agriculture in the United States.

Overall, the principles proposed in this US self-regulation document establish a rural data protection framework in some respects similar to the European model of personal data protection. We present the main provisions established by this self-regulation model below:

- a) The ownership of the data generated by rural operations belongs to the agricultural producer. However, it is the producer's responsibility to agree to use and sharing of this data with other stakeholders who have economic interests, such as lessees, landowners, cooperatives, owners of precision agriculture system hardware and/or agricultural technology providers;
- b) Rural data collection, access and use must only occur after obtaining the producer's affirmative and explicit consent;
- c) The agricultural technology provider must explain the effects and possibilities of the producer's choice to opt-in, opt-out or disable the availability of the offered services and functionalities;
- d) Producers must be informed if their data is being collected and how rural data will be made available and used. This information must be easily accessed and provided in an accessible format;
- e) Agricultural technology providers must inform the producers regarding the purposes for which rural data is being collected and used. Among the necessary information, there must be contact information to ask questions and register complaints, information on what type of third parties will have access to the data and the alternatives offered by the provider for the producer to limit its use and availability. The agricultural technology provider will not change the terms of the contract without the client's consent;
- f) In the context of the contract and the data retention policy, producers must be able to migrate their rural data and store or use them in other systems. This rule does not apply to data that has already been anonymized or aggregated;
- g) The agricultural technology provider may not sell and/or disclose non-aggregated data to a third party without previously establishing a binding agreement to ensure that the third party will comply with the same terms and conditions the provider has established with the producer. Producers must also be informed that the sale will maintain their option to opt-out or exclude their data prior to the sale. The agricultural technology provider will not share or disclose original rural data with/to a third party in a way that does not honor the contract established with the producer;
- h) Agricultural technology providers must promote the removal, safe destruction and return of original rural data to the agricultural producer's account, by the producer's request or following a previously established timeframe;
- i) Farmers must have the possibility of discontinuing the data collection service at any time, subject to ongoing obligations;

- j) The agricultural technology provider must not use rural data in illegal or anti-competitive activities. For example, the agricultural technology provider is prohibited from using rural data for speculating on the commodities market;
- k) Rural data must be protected by reasonable security standards, in order to avoid risks regarding the loss, change, destruction or non-authorized access to data. There must also be a clear policy to inform and respond to cases of data leaks.

In the same context of the AFBF principles, the European COPA-COGECA<sup>dxxi</sup> published a document in which it recommends principles for the handling of rural data, with many interfaces and similar to the principles established by AFBF.<sup>dxxi</sup>

On the other hand, the Brazilian Association of Seeds and Plants (“ABRASEM”) has been advocating for a more liberal position regarding the debate on rural data within Congress.

During the July 12, 2017 public hearing at the Congressional Special Committee on Data Protection, ABRASEM indicated that the current Bills have provisions place innovations on precision agriculture industry at risk, resulting in a loss of national competitiveness. Among these, the committee noted: a) lack of clarity on some concepts related to the agricultural scenario; b) restrictions presented by the Bills for international transfer of data; c) impediments for innovation in the precision agriculture industry; d) equal treatment for different industries, such as precision agriculture.

In ABRASEM’s contribution to Bill no. 5.276/2016,<sup>dxiii</sup> one can identify, for example, the industry’s concern with the application of the Bill’s concept of personal data in the handling of georeferenced data, since georeferencing is one of the fundamental principles of precision agriculture.<sup>dxiv</sup>

Other than these two large groups, it is also important to mention the academic debate raised by the Research Group for Teaching and Innovation (“GEPI”) at the Getúlio Vargas Foundation (“FGV”) Law School in São Paulo. In a recently published research on precision/digital agriculture,<sup>dxv</sup> GEPI determined that a portion of data in the rural environment related to personal data. This would enable the identification or the possibility of identifying the producer as a private individual through data.

Therefore “assuming that there is no personal data in agriculture” would be, in the Group’s opinion, a contradiction. However, according to the analysis, although personal data is present in the rural environment, it is not “as significant” or important, especially if compared to the dynamics and logic of other environments, such as Health and Cities.

In our opinion, there appear to be two different debates that will require complementary approaches: I) the application of the legal framework for personal data; and II) possession and protection of non-personal data or, in other words, data related to the rural economic activity.

Regarding the application of the legal framework to personal data (current or future) for IoT data, we find that it would only happen in specific situations and that it does not represent an obstacle to the development of IoT in the rural environment since, in these cases, there would only

be a requirement to comply with the regulations for handling of personal data. However, the majority of rural IoT applications do not involve personal data (related to an identified or identifiable private individual), but non-personal data related to the agribusiness economic activity, with specific topics to be addressed, such as ownership and protection.

This last topic is the focus of a second debate, which remain unresolved in Brazil and will need to be further developed by interested actors to identify possible approaches to address the concerns of all stakeholders. One solution could be to centralize it at the CBAP, which features the widespread participation of key industries on the topic of IoT in the rural environment.

The models presented, considering both the principles of the AFBF and of COPA-COGECA, are precisely directed at how to regulate issues involving the ownership and protection of non-personal data in the rural environment. In our opinion, these models may serve as examples for the developing debate, in order to promote both innovation and to guarantee the protection of the individual producer in terms of non-personal data generated by their activities.



- 
1. <sup>i</sup>Available at: <http://participa.br/cpiot>.
  2. <sup>ii</sup>The issue of expanding the exemption of the Telecommunications Inspection Fund (“FISTEL”) will be addressed as a separate item.
  3. <sup>iii</sup>See, for example, Bill no. 7.656/2017 (authored by Congressmen Vitor Lippi and Odorico Monteiro, commented by ANATEL). Available at [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw\\_9INcO4F5XiKYL1f8c-OplHKiusgnFeAtzDzvx7FNVI3h9VcWTOBPVj8nMPmHyacWmvXhRWWvB6-7AFm8UjEQ6ccchyVg](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4F5XiKYL1f8c-OplHKiusgnFeAtzDzvx7FNVI3h9VcWTOBPVj8nMPmHyacWmvXhRWWvB6-7AFm8UjEQ6ccchyVg)
  4. <sup>iv</sup>See, for example, Bill no. 7.656/2017 (authored by Vitor Lippi and Odorico Monteiro, with comments from ANATEL). Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw\\_9INcO4F5XiKYL1f8c-OplHKiusgnFeAtzDzvx7FNVI3h9VcWTOBPVj8nMPmHyacWmvXhRWWvB6-7AFm8UjEQ6ccchyVg](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4F5XiKYL1f8c-OplHKiusgnFeAtzDzvx7FNVI3h9VcWTOBPVj8nMPmHyacWmvXhRWWvB6-7AFm8UjEQ6ccchyVg)
  5. <sup>v</sup>Germany. Definition of M2M communication adopted by German authorities available at: [https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/TechnicalNumbers/IMSI\\_Extra-territorial.pdf?\\_\\_blob=publicationFile&v=1](https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/TechnicalNumbers/IMSI_Extra-territorial.pdf?__blob=publicationFile&v=1).
  6. <sup>vi</sup>Definition of M2M published by the Telecommunications Commission of Canada, available at: [http://www.crtc.gc.ca/eng/dcs/current/faq\\_43.htm#a13](http://www.crtc.gc.ca/eng/dcs/current/faq_43.htm#a13).
  7. <sup>vii</sup>On the subject of reversibility of assets, it is worth mentioning that Ordinance no. 1.455/2016 of the Ministry of Communications, which establishes the guidelines for ANATEL in regard to the revision of the service provision model, is manifested by the need to remove this institute. Available at: <http://www.anatel.gov.br/legislacao/normas-do-mc/899-portariamc-1455>. Accessed on 09/12/17.
  8. <sup>viii</sup>It is worth noting as an example, the already mentioned replacement to Bill no. 7.406/2014, as reported by Congressman Jorge Tadeu Mudalen. Available at: [http://www.camara.gov.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1509928&filename=PRL+5+PL740614+%3D%3E+PL+7406/2014](http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1509928&filename=PRL+5+PL740614+%3D%3E+PL+7406/2014). Accessed on 18/09/17.
  9. <sup>ix</sup>According to a recent analysis made by the Court of Audit of the Union (TCU – [decision 749/2017](#)), only 0.002% of FUST resources were allocated for universal access of telecommunication services. In addition, 84% of the resources raised from 2001 to 2016 for FUST (approximately 17.2 billion *reais*) have already been used by the government for other purposes. Available at: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15B4A7944015B6411539954CA&inline=1>. Accessed on 20/11/2017.
  10. <sup>x</sup>Public consultation on the National Connectivity Plan started on October 18, 2017 and ended on November 17, 2017.

- 
11. <sup>xI</sup>ANATEL Resolution no. 617/2013, art. 3: “PLS is a telecommunication service of restricted interest, operating on a national and international level, in the private regime, for the use of the service provider or provided to a determined user group, selected by the provider according to criteria established by it, which covers multiple applications, among which the communication of data, video and audio, voice and text signals, as well as the capture and transmission of Scientific Data related to Exploration of the Earth by Satellite, Assistance to Meteorology, Meteorology through Satellite, Space Operations and Space Research.”
12. <sup>xII</sup>Former ANATEL Resolution no. 506/2008, Article 3.
13. <sup>xIII</sup> Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?cEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw\\_9INcO5qKCcRSzoq5DnXXPJm9hKqzeSvGfpxp0Fu\\_WoFxlJ6rIRaCNKvC4RxM8uXVPEEW7BqBFNjtRWtYXl9RgoVX-6t](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?cEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5qKCcRSzoq5DnXXPJm9hKqzeSvGfpxp0Fu_WoFxlJ6rIRaCNKvC4RxM8uXVPEEW7BqBFNjtRWtYXl9RgoVX-6t)
14. As an example, see the change in ANATEL Resolution no. 663/2016 which excludes the limitation for Accredited MVNOs of controlling, being controlled by or affiliated to other Accredited MVNOs in the same geographic area.
- xiv
15. <sup>xv</sup> “How to become a MVNO Operator”, available at: <http://www.anatel.gov.br/grandeseventos/pt-br/como-se-tornar-um-operador-mvno>
16. <sup>xvi</sup> ANATEL, Directive Release no. 98/2015/SEI/PRRE/SPR-ANATEL. Available at: [https://sei.anatel.gov.br/sei/modulos/pesquisa/md\\_pesq\\_documento\\_consulta\\_externa.php?WwIhLN\\_g9R51QStF7kKYBHkoN4GOioaWR9LFGBGK627HLLXn0lySP5NvKOPPiWBvcaCzM3y0c3MOWE17vym14WMYQxiqVWaEwKY0c6tjm1UJcY093WgCCImLUr7hpXU](https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?WwIhLN_g9R51QStF7kKYBHkoN4GOioaWR9LFGBGK627HLLXn0lySP5NvKOPPiWBvcaCzM3y0c3MOWE17vym14WMYQxiqVWaEwKY0c6tjm1UJcY093WgCCImLUr7hpXU) .
17. <sup>xvii</sup> “The unblocking of the Mobile Station is a right of the PMS user and may be exercised at any time before the Provider responsible for the block, and it is forbidden to charge any amount from the user for this service” Available at: <http://www.anatel.gov.br/legislacao/sumulas/60-sumula-8>
18. <sup>xviii</sup> For more information, please see: <https://www.gsma.com/rsp/>
19. <sup>xix</sup> The issue was addressed by the Agency in Directive Release no. 43/2012/PVCP/PR/CP, of June 28 of 2012, as a response to questions on the regularity of the use of mobile terminals through a SIM card and numbering resources from foreign providers, in order to offer VAS permanently to residents of Brazil. In addition, ANATEL manifested itself on this in a meeting of the Economic Policy Commission (SG3) of the International Communication Union (“ICU”), when it stated that “permanent roaming could cause an unbalance in competition, since a global telecommunications operator would be created and would not pay local business taxes”. Information available at: <http://www.telesintese.com.br/brasil-diz-nao-ao-roaming-permanente/> .
20. <sup>xx</sup> Although it does not address international roaming, it is worth noting that Directive Release no. 1/1998 from ANATEL includes a requirement for signing a roaming agreement with other operators in case this option is offered by a specific operator. This understanding also applies to international roaming agreements, reinforcing the viability of regulatory model adopted by the Agency.
21. RAMOS, Marcelo de Matos; LIMA Marcelo Sá Leitão Fiuza. *Sobre o uso eficiente do espectro radioelétrico*. Available at: [http://seac.fazenda.gov.br/central-de-documentos/documentos-de-trabalho/documentos-de-trabalho-2006/DT\\_42.pdf](http://seac.fazenda.gov.br/central-de-documentos/documentos-de-trabalho/documentos-de-trabalho-2006/DT_42.pdf).
- xxi
22. <sup>xxii</sup> Index specifications, information collection, calculations and other matters related to quality requirements may be found in the following regulations: (i) annex of Resolution no. 574/2011, regarding MCS; (ii) annex of Resolution no. 575/2011, regarding PMS; (iii) annex of Resolution no. 605/2012, regarding FSTS; (iv) annex of Resolution no. 411/2015, regarding TSCI. Other than that, it is worth mentioning Resolution no. 654/2015, which has approved the Regulation on the Measurement of Degree

---

of Satisfaction and of the Quality Perceived by Telecommunication Users. Devices included in this Regulation apply to providers of PMS, MCS, FSTS and pay television.

23. <sup>xxiii</sup>Regarding condition of equality imposed by QMRs, which brings quality goals to be observed by providers of PMS and MCS. In these regulations, the wordings of respective arts. 1st, paragraph 3, establish that goals related to the network and to users must be equally met by all providers – with exception only of those considered as small businesses.
24. <sup>xxiv</sup>It is the case of the minimum index of successful attempts of connection to the data network (art. 20 of QMR/PMS), as well as of the minimum bidirectional latency of 80 milliseconds for 95% of the cases (art. 18 of QMR/MCS), that correspond to quality indexes for any connection.
25. <sup>xxv</sup>Available at:  
<https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2036&Tipo=1&Opcao=andamento>
26. <sup>xxvi</sup>According to GSMA, “M2M connections usually generate significantly lower ARPU in comparison to personal connections, therefore the reduction of taxes related to M2M should represent an important role in the development of the market.” Available at:  
[https://www.gsma.com/mobileeconomy/archive/GSMA\\_ME\\_Latam\\_2014.pdf](https://www.gsma.com/mobileeconomy/archive/GSMA_ME_Latam_2014.pdf) . Accessed on 09/15/17.
27. <sup>xxvii</sup>It is also worth mentioning that the cost for data use in Brazil is being significantly reduced. According to numbers from ANATEL, from 2010 to 2015, the average monthly value of 1Mbps has decreased by 71.7%, going from R\$ 21.18 to R\$ 5.98. Other than that, ANATEL has registered a decrease of 53.9% in the ARPU of mobile telephony from the first trimester of 2009 to the second trimester of 2015. For more information, please see:  
<http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=342736&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=342736.pdf>,  
<https://cloud.anatel.gov.br/index.php/s/VxuWaQltgEeQKyU/download?path=%2F&files=Relat%C3%B3rio%20de%20acompanhamento%20SMP%20-%201T16.pdf> and  
<http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=316693&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=316693.pdf>
28. <sup>xxviii</sup>Bill no. 7,656/2017, status available at:  
<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2137811> .
29. <sup>xxix</sup>ANATEL Case no. 53500.060180/2017-61, Report no. 57/2017/SEI/PRRE/SPR.
30. <sup>xxx</sup>ANATEL Case no. 53500.060180/2017-61, Report no. 57/2017/SEI/PRRE/SPR.
31. <sup>xxxi</sup>General Telecommunications Law, art. 60.
32. <sup>xxxii</sup>General Telecommunications Law, art. 61.
33. <sup>xxxiii</sup>The objective in this work is not to study the constitutionality of ISS on software licensing. In fact, the matter is being judged by the Superior Federal Court, under the scope of the Extraordinary Appeal no. 688.223.
34. <sup>xxxiv</sup>IoT activities involve multiple taxes on consumption e.g., Import Tax ("II"), Industrialized Products Tax ("IPI"), ICMS, Contribution to the Social Integration Program ("PIS" ("Cofins") and ISS, as well as sector fees and contributions (contributions to FUST, FUNTTEL and FISTEL).
35. <sup>xxxv</sup>Available at  
[http://www.doingbusiness.org/~/\\_media/wbg/doingbusiness/documents/profiles/country/bra.pdf](http://www.doingbusiness.org/~/_media/wbg/doingbusiness/documents/profiles/country/bra.pdf).  
Accessed on March 16, 2017.
36. <sup>xxxvi</sup>The average in OECD countries is 163.4 hours. Brazil is in last place.

- 
37. <sup>xxxvii</sup> According to OECD (2015), *Addressing the Tax Challenges of Digital Economy, Action 1 -2015*. Final Report OECD/G20, Base Erosion and Profit Shifting Project, OECD Publishing, Paris. Available at: <http://dx.doi.org/10.1787/9789264241046-en>. Accessed on: March 16, 2017.
38. <sup>xxxviii</sup> According to OECD (2015), *Addressing the Tax Challenges of Digital Economy, Action 1 -2015*. Final Report OECD/G20, Base Erosion and Profit Shifting Project, OECD Publishing, Paris. Available at: <http://dx.doi.org/10.1787/9789264241046-en>; p. 100-101. Accessed on March 16, 2017.
39. <sup>xxxix</sup> Task Force on Taxation of the Digital Economy. Collin Pierre, Colin Nicolas. Jan./2013, p. 35 and ss. Available at: [https://www.hldataprotection.com/files/2013/06/Taxation\\_Digital\\_Economy.pdf](https://www.hldataprotection.com/files/2013/06/Taxation_Digital_Economy.pdf).
40. <sup>xl</sup> Defined in Article 544 of Decree no. 3.000, of March 26, 1999.
41. <sup>xli</sup> The SUDENE regions are established in Supplementary Law no. 125, January 3, 2007. The SUDAM regions were established through Supplementary Law no. 124, of January 3, 2017.
42. <sup>xlii</sup> Regarding the topic, on April 18, 2017, Gileno Barreto and Antonio Rocca published an article in *Valor Econômico*: "It is important to initially mention that from the point of view of fiscal incentives, Brazilian legislation is relatively efficient compared to other countries. Data from the OECD's 2013 R&D and Tax Incentives Report shows that the Good Law puts Brazil in the 9th-place position in volume of subsidies. However, in a scenario of losses - which usually occurs in times of crisis - Brazilian legislation takes us to the 20th position, as it does not provide for the possibility of deferment of the incentive for other years (...) Brazil can no longer waste time. Industry 4.0 is knocking at our door, the "Internet of Things" is advancing in developed countries. We have a good legal model of incentives for innovation that needs a few but significant adjustments that will provide the private sector with the legal security necessary to get projects off the back burner and become a reality."
43. <sup>xliii</sup> Regulated by Decree no. 288, of February 28, 1967, approved by the Federal Constitution of 1988. Tax incentives are provided for until 2073, according to Constitutional Amendment no. 83/2014.
44. <sup>xliv</sup> The region is divided into 3 "sub-regions": (i) Manaus Free Zone ("ZFM"), (ii) Western Amazon ("AMOC") e (iii) Free Trade Areas ("ALC").
45. <sup>xlv</sup> For example, advantages due to location, as seen in [http://www.suframa.gov.br/zfm\\_incentivos.cfm](http://www.suframa.gov.br/zfm_incentivos.cfm).
46. <sup>xlv</sup> The PPB is the minimum set of operations in the manufacturing establishment, which characterizes the effective industrialization of a certain product, being established by the State Ministries of Development, Industry and Foreign Trade and Science and Technology. The PPB applicable for the Manaus Free Trade Zone was established by Law 8.371, of December 30, 1991 and is regulated by Decree No. 6.008 of December 23, 2006.
47. <sup>xlvii</sup> The Promise and the Peril of Data-Driven Society, article published by *The New York Times* in 02.25.2013, the concept of data-driven societies is discussed, addressing the impact of big data on social media, business decisions and matters of online privacy. Available at: [https://bits.blogs.nytimes.com/2013/02/25/the-promise-and-peril-of-the-data-driven-society/?\\_r=0](https://bits.blogs.nytimes.com/2013/02/25/the-promise-and-peril-of-the-data-driven-society/?_r=0). Accessed on 08.21.2017.
48. <sup>xlviii</sup> According to *The Economist* magazine, in May 2017, the same legislative concerns that existed in the previous century with the oil industry repeat themselves with the rising of large companies of the digital world. The control these companies have over their users' data grants them great economic power. With the increase of devices connected to the Internet, the volume of data owned by these companies tends to grow exponentially. Available at: <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>. Accessed on 08.18.2017.
49. <sup>xlix</sup> The different techniques of handling and analyzing data enable the availability of a series of functionalities and digital services, among which are digital advertising and use of big data by telephone companies to support public administration. More information at: <http://www.inova.jor.br/2017/08/07/big-data-telecomunicacoes-cidades/>. Accessed on 08.21.2017.

- 
50. <sup>l</sup>HIRSCH, Dennis D. The Law and policy of online privacy: Regulation, self-regulation, or co-regulation? 34 Seattle U. L. Rev. 439, 2010-2011, p. 451.
51. <sup>li</sup>KLEINSTEUBER, Hans. J. Self-regulation, co-regulation and state regulation, p. 62. Available at: <http://www.osce.org/fom/13844?download=true>. Accessed on 08.25.2017.
52. <sup>lii</sup>POULLET, Yves. How to regulate Internet: New paradigms for Internet governance self-regulation: Values and limits. 1999, p. 84-88. Available at: <http://www.crid.be/pdf/public/4656.pdf>. Accessed on 08.25.2017.
53. <sup>liii</sup>The National Advertising Self-Regulating Council (CONAR) is a Brazilian example.
54. <sup>liv</sup>See *Selfregulation.info*. Available at: <http://www.law.uni-sofia.bg/Kat/T/IP/T/PM/DocLib/Internet%20Self-Regulation%20An%20Overview.htm>. Accessed on 08.28.2017.
55. <sup>lv</sup>For Kleinsteuber, if the State and private regulators cooperate in joint institutions, there is co-regulation (p. 63). According to Christopher T. Marsden, co-regulation includes a variety of different regulatory phenomena, with the commonality being the fact that the regulatory regime is structured from a complex interaction between current legislation and auto-regulating entities. The many interests of these actors result in different incentives for them to cope. In: Internet Co-regulation and Constitutionalism: Towards a More Nuanced View. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1973328&rec=1&srcabs=1988369&alg=1&pos=1](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1973328&rec=1&srcabs=1988369&alg=1&pos=1). Accessed on 08.25.2017.
56. <sup>lvi</sup>MARSDEN, Christopher T. Internet co-regulation and constitutionalism: Towards a More Nuanced View. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1973328](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1973328). Accessed on 08.31.2017.
57. <sup>lvii</sup>RODRIK, Dani. Institutions for High-Quality Growth: What They Are and How to Acquire Them. Cambridge: NBER, 2000 (Working Paper, no. 7,540). Available at: <http://www.nber.org/papers/w7540>. Accessed on 08.26.2017.
58. <sup>lviii</sup>United States Chamber of Commerce; Hunton & Williams LLP. Seeking solutions: Attributes of Effective Data Protection Authorities, 2016. Available at: [https://www.uschamber.com/sites/default/files/023052\\_dataprotectionhuntonpaper\\_fin.pdf](https://www.uschamber.com/sites/default/files/023052_dataprotectionhuntonpaper_fin.pdf). Accessed on 08.23.2017.
59. <sup>lix</sup>In 1999, *Bertelsmann Foundation* indicated the need to involve private actors in state enforcement practices due to the government's lack of capacity to deal with the changing global and technical nature of the virtual environment. Moreover, the suggestion is that Internet intermediates be considered potential allies, to promote governance and to avoid network irregularities. Bertelsmann Foundation. Self-regulation of Internet Content, 1999, p. 49. Available at: <https://cdt.org/files/speech/BertelsmannProposal.pdf>. Accessed on 08.25.2017.
60. <sup>lx</sup>GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. Available at: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Accessed on 08.21.2017.
61. <sup>lxi</sup>Ibid., p. 19-24.
62. <sup>lxii</sup>European Council (EC) and European Court of Human Rights (ECHR) Guidebook on Data Protection European Legislation, 2014, p. 18. Available at: <https://rm.coe.int/16806ae65f>. Accessed on August 29, 2017.
63. <sup>lxiii</sup>The Directive determines general rules on the legitimacy and limits of personal data handling and stipulates the rights of data subjects and provides for national independent supervision authorities. More information at:

- 
- [http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU\\_5.12.8.html](http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU_5.12.8.html). Accessed on August 29, 2017.
64. <sup>lxiv</sup>To review the history of Internet regulation of the European Union, see FEELEY, Matthew J. EU Internet Regulation Policy: The Rise of Self-regulation, 22 B.C. Int'l & Comp. L. Rev. 159 (1999). Available at: <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1216&context=iclr>. Accessed on August 29, 2017.
65. <sup>lxv</sup>The General Data Protection Resolution features the co-regulation model, in which the public power establishes vast normative standards for the protection of rights, while, at the same time, allows private initiative to establish private regulations on the technological sector. As seen in [https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-regulacao-da-transferencia-transnacional-de-dados-06072017#\\_edn3](https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-regulacao-da-transferencia-transnacional-de-dados-06072017#_edn3). August 29, 2017.
66. <sup>lxvi</sup>Articles 7 and 8 of the Charter recognize the respect for private life and personal data protection as distinct but closely related fundamental rights. The Charter is part of the Lisbon Treaty, which establishes certain principles for privacy protection and is legally binding in institutions and organs of the Union and of the Member States when European Union legislation is applied.
67. <sup>lxvii</sup>Its tasks are specifically defined in Article 30 of Directive no. 95/46/CE and Article 15 of Directive no. 2002/58/EC.
68. <sup>lxviii</sup>More information on Article 19 Working Group at: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083). Accessed on 08.29.2017.
69. <sup>lxix</sup>More information on European Data Protection Board at: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en). Accessed on 29.10.2018.
70. <sup>lxx</sup>More information on European Commission at: [https://europa.eu/european-union/about-eu/institutions-bodies/european-commission\\_en](https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en). Accessed on 29.10.2018.
71. <sup>lxxi</sup>Available at: <http://ec.europa.eu/dpo-register/search.htm>. Accessed on 08.29.2017.
72. <sup>lxxii</sup>The Federal Trade Commission was created in 1914 with the signing of the Federal Trade Commission Act. It is an independent governmental agency, led by five commissioners named by the President of the US and confirmed by the Federal Senate for seven years. Its primary objectives are consumer protection and the assurance of market competition. More information at: <https://www.ftc.gov/about-ftc/our-history>; <https://www.law.cornell.edu/uscode/text/15/41>. Accessed on August 28, 2017.
73. <sup>lxxiii</sup>“Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful” [15 U.S.C. paragraph 45(a)].
74. <sup>lxxiv</sup>Within the reasons for initiating an investigation process are consumer complaints, internal research, recommendations from organizations of the civil society or from the private sector, news published by the media, and public policy priorities. More information at: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/Estados-Unidos-Anexos.pdf>. Accessed on August 28, 2017.
75. <sup>lxxv</sup>More information at: [https://www.americanbar.org/groups/young\\_lawyers/publications/the\\_101\\_201\\_practice\\_series/understanding\\_differences.html](https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/understanding_differences.html) and <https://www.law.cornell.edu/uscode/text/15/45>. Accessed on August 28, 2017.
76. <sup>lxxvi</sup>BOWIE, Norman E.; JAMAL, Karim. Privacy Rights on the Internet: Self-regulation or Government regulation? Business Ethics Quarterly, Vol. 16, No. 3 (July 2006), pp. 323-342. Available at: <http://www.jstor.org/stable/3857919>. Accessed on 08.26.2017. In a research led by the authors (p. 332) on the 100 selected high traffic electronic addresses, 34 had a certification seal. All of these 34 websites and 63 more (from a total of 66 websites that did not have one) have a privacy policy.

- 
77. <sup>lxxvii</sup>SOMBRA, Thiago. A regulação da transferência transnacional de dados. JOTA, 07.06.2017. Available at: <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-regulacao-da-transferencia-transnacional-de-dados-06072017>. Accessed on 08.28.2017.
78. <sup>lxxviii</sup>Convention 108 of the Council of Europe for the Protection of Individuals is the first legally binding international instrument adopted within the context of data protection. It aims to guarantee all individuals respect to their fundamental rights and liberties and especially the right to a private life, before the automated handling of personal data. More information at: [http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU\\_5.12.8.html](http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU_5.12.8.html). Accessed on August 31, 2017.
79. <sup>lxxix</sup>LPDP was regimented by Decree no.414, of 2009.
80. <sup>lxxx</sup>GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais, p. 22. Available at: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Accessed on August 21, 2017.
81. <sup>lxxxi</sup>In Spanish, *Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento*.
82. <sup>lxxxii</sup>Available at: <https://www.datospersonales.gub.uy/inicio/Resoluciones+y+dictámenes/dictámenes/>. Accessed on August 30, 2017.
83. <sup>lxxxiii</sup>Available at: <https://www.datospersonales.gub.uy/inicio/publicaciones/Guias+de+ayuda/>. August 30, 2017.
84. <sup>lxxxiv</sup>As described in detail in Decree no. 414/2009.
85. <sup>lxxxv</sup>Among such characteristics are agility and flexibility, meaning the ability to react to new technologies and new business models; technical expertise; stability and long-term vision; cooperative relationship with the private sector, society and the government; institutional articulation with, for example, foreign authorities and multinational companies, considering the transnational dimension of the market.
86. <sup>lxxxvi</sup>InternetLab, O que está em jogo no debate sobre proteção de dados pessoais no Brasil? 2016, p. 18-19. Available at: [http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta\\_apl\\_dados\\_pessoais\\_final.pdf](http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf). Accessed on 08.25.2017. This report was based on contributions sent to the Ministry of Justice through a platform named “Pensando o Direito” during the entire period of the Bill’s public hearing, from January 28 to July 5 of 2015.
87. <sup>lxxxvii</sup>Research Group on Public Policies for Information Access at the University of São Paulo has suggested that States, the Federal District and Cities must be able to create their own authorities of personal data protection with concurrent competencies and within their own operation areas. *Ibid.*, p. 24-25.
88. <sup>lxxxviii</sup>To access the actors’ contributions to the institutional design of the protection authority from the Congressional public consultation on Bills no. 4.060/2012 and no. 5,276/2016 on 05.31.2017, see: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-publicas>. Accessed on 08.31.2017.
89. <sup>lxxxix</sup>*Ibid.*, p. 18-19.
90. <sup>xc</sup>As personal data protection may be stipulated as a fundamental right in the Constitution (sanctity of privacy, private life, honor and image of people, in article 5, X), it would entail some state involvement.
91. <sup>xci</sup>As in the United States, where sector regulations issued by agencies co-exist with self-regulatory mechanisms.



- 
92. <sup>xcir</sup>This was the first proposal of the Center for Society and Technology at the Getúlio Vargas Foundation (CTS-FGV), which has suggested the creation of an autarchy or a national system of personal data protection. In: InternetLab, O que está em jogo no debate sobre proteção de dados pessoais no Brasil? 2016, p. 20. Available at: [http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta\\_apl\\_dados\\_pessoais\\_final.pdf](http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf). Accessed on 08.25.2017.
93. <sup>xciii</sup>Ibid., p. 441. Kamara (2017) affirms that the rising of new technologies brings the need to think of auto and co-regulation models to establish technical standards for personal data protection. However, auto-regulation is seen as a limited mechanism, for being flexible and guided by the market may lead to the promotion of interests regarding only private groups. In: KAMARA, Irene. Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardization 'mandate'. European Journal of Law and Technology, Vol. 8, No. 1, 2017.
94. <sup>xciv</sup>Cf. Law no. 10,848/2004, Decree no. 5,177/2004 and Normative Resolution no. 109/2004.
95. <sup>xcv</sup>Suggestion presented in public hearing by the Society and Technology Institute. There are different points of contention related to personal data protection and the publishing of public data bases, and they will be addressed in this publication.
96. <sup>xcvi</sup>In 2013, the agency raised 22 million euros through fines, with its costs corresponding to 13 million euros in that year. The excess amount is directed to the National Treasury. InternetLab, O que está em jogo no debate sobre proteção de dados pessoais no Brasil 2016, p. 23. Available at: [http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta\\_apl\\_dados\\_pessoais\\_final.pdf](http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf). Accessed on 08.25.2017.
97. <sup>xcvii</sup>Regarding this issue, it is important to allocate distribution of funds raised by fines, so that the monies do not go to generic or contingency funds.
98. <sup>xcviii</sup>A model similar to Uruguay's is United Kingdom's, which requires the mandatory registry of data controllers. The Data Protection Act of 1998 requires that any organization that processes personal information registers before the Information Commissioner's Office (ICO), under penalty of configuring as a criminal offense. Available at: <http://www.legislation.gov.uk/ukpga/1998/29/contents>. Accessed on 08.31.2017.
99. <sup>xcix</sup>According to <https://goo.gl/1dmeDq>.
100. <sup>c</sup>For more information on the ecosystem of attacks on IoT devices, we suggest consulting the Guidelines for Internet Security 4.0 (*Cartilha de Segurança para Internet v.4.0*), published by the Center for Studies, Response and Treatment of Security Incidents in Brazil ("CERT.br"). Available at <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. For more information on the attacks in Brazil in 2017, access: <http://cio.com.br/noticias/2018/01/31/brasil-sofreu-264-9-mil-ataques-ddos-em-2017-35-gerados-no-proprio-pais/>.
101. <sup>ci</sup>It is worth noting that the topic of information security is already contained in the Declaration of Principles at the World Summit on the Information Society in 2003. See World Summit on the Information Society Documents: Geneva 2003 and Tunis 2005/ International Telecommunication Union. São Paulo: Internet Steering Committee in Brazil, 2014.
102. <sup>cii</sup>Despite criticism regarding the possibility of including the ITU agenda in an international instrument by the ITU, the agency acts positively in several aspects related to the subject. The branch of the agency responsible for standardization (ITU-T) has issued hundreds of technical standards on information security, which is positive for private initiative. In parallel, ITU assists developing countries in the creation of Network Incident Handling Centers. See <https://www.itu.int/en/wcit-12/Documents/WCIT-background-brief6.pdf>.
103. <sup>ciii</sup>Available at <https://www.cept.org/Documents/com-itu/7628/>.
104. <sup>civ</sup>European Union Agency for Network and Information Security (ENISA), 2015, Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, v. 1.0.



- 
105. <sup>cv</sup>Available at [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf).
106. <sup>cvi</sup>The issue has already been the subject of questioning in the House Chamber. Requests REQ 307/2013 CREDN (filed), RIC 3.464/ 2013 (archived), RIC 3.465/2013 (archived), solicit information on Brazil's accession to the Convention on Cybercrime. In parallel, Bills 3.175 /2012 and 4.424/2008, provide for the amendment of the Criminal Code to harmonize the national legal system with the Convention.
107. <sup>cviir</sup>To a great extent the Convention on Cybercrime influenced Bill No. 84/1999, proposed by Senator Eduardo Azeredo and which was rejected by majority vote. The bill created widespread public debate, including online petition with tens of thousands of signatures opposing its approval. Congress initiated discussion in the Legislative Branch, coming to the conclusion that a criminal bill could not be considered the best option to regulate the internet in Brazil.
108. <sup>cviir</sup>The Federal Constitution of 1988, available at: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm).
109. <sup>cix</sup>For an overview of the Agreements on Mutual Protection and Exchange of Classified Information, see FORNAZARI JÚNIOR, M. PF em pauta – Cooperação jurídica internacional, available at <https://jota.info/artigos/pf-em-pauta-cooperacao-juridica-internacional-17032016>. For details about permitted diligences and necessary requirements for concession, see the Guide for International Legal Cooperation in Criminal Matters, published by the Department of Asset Recovery and International Legal Cooperation of the Ministry of Justice. Available at: <http://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf>.
110. <sup>cx</sup>See Access Now – Mutual Legal Assistance Treaties - Policy Analysis, available at <http://mlat.info/policy-analysis>.
111. <sup>cx</sup>For an illustration of the challenges involved in obtaining information for requests for assistance, see FORCE HILL, J. Problematic Alternatives: MLAT Reform for the Digital Age, Harvard Law School, National Security Journal, 2015. Available at: <http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/>. Accessed on October 9, 2017.
112. <sup>cxii</sup>Available at: <http://www.mcti.gov.br/documents/10179/2100710/04.08+Estrat%C3%A9gia+Brasileira+para+Transforma%C3%A7%C3%A3o+Digital/cdbc34bf-c9d0-48ae-a8aa-aa4b4b4886af>.
113. <sup>cxiii</sup>Legislative Decree no. 272/2007, available at: <http://legis.senado.gov.br/legislacao/ListaTextoIntegral.action?id=235170&norma=256138>.
114. <sup>cxiv</sup>See, as reference, KELLO, LUCAS. The Virtual Weapon and International Order. NEW HAVEN; LONDON, Yale University Press, 2017; TROPÍNA, T., CORMAC C. Self-and Co-regulation in Cybercrime, Cybersecurity and National Security. Heidelberg: Springer, 2015; WEBER, R. Governance of the Internet of Things – From Infancy to Frist Attempts of Implementation? Laws, v. 5, n. 3, p. 28, 2016.
115. <sup>cxv</sup>NETMundial, The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness, available at <http://content.netmundial.br/contribution/the-importance-of-a-multistakeholder-approach-to-cybersecurity-effectiveness/180>.
116. <sup>cxvi</sup>See the position of Microsoft, available at <https://blogs.microsoft.com/microsoftsecure/2017/06/07/nist-cybersecurity-framework-building-on-a-foundation-everyone-should-learn-from/>.
117. <sup>cxvii</sup>In the European Union, the need to create a multisectoral environment is reflected in the Cybersecurity Strategy published in 2013. See European Commission, European Union Strategy for Cybersecurity: an Open, Secure and Protected Cyberspace, JOIN(2013) 1 final, available at [http://www.dgpi.mj.pt/sections/informacao-e-eventos/2013/encontros-de-direito/downloadFile/attachedFile\\_3\\_f0/ESTRATEGIA\\_EUROPEIA\\_CIBERSEGURANCA.pdf?nocache=1400574470.82](http://www.dgpi.mj.pt/sections/informacao-e-eventos/2013/encontros-de-direito/downloadFile/attachedFile_3_f0/ESTRATEGIA_EUROPEIA_CIBERSEGURANCA.pdf?nocache=1400574470.82). The position is aligned with that of the World Economic Forum, according to the

---

document “Global Agenda Council on Cybersecurity”, available at [www3.weforum.org/docs/GAC16\\_Cybersecurity\\_WhitePaper .pdf](http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper.pdf).

118. <sup>cxviii</sup>Article 61, Paragraph 1, subsection II, line e, of the Federal Constitution of 1988 establishes that the law regarding creation of organs of the public administration is the exclusive responsibility of the President of the Republic.
119. <sup>cxix</sup>The use of Internet of Things devices involves a number of information security risks, given the scenario in which consumers are unaware of the technical peculiarities of the devices and, as a consequence, the resulting security risks. Some cases are paradigmatic of this scenario. For a comprehensive overview, see LEVERETT, E. CLAYTON, R. ANDERSON, R. "Standardisation and Certification of the 'Internet of Things'" (2017).
120. <sup>cxx</sup>In a paradigmatic illustration of the impact of non-compliance of security criteria for Internet-connected devices in 2016, unprotected objects such as security cameras, cable TV converters, routers, digital television recorders and the like were used in denial of service attacks. Data traffic from millions of objects was used to attack US corporate servers. The objects used by the attack shared the same characteristics: low cryptographic protection, no password protection, or use of standard passwords (such as "admin, admin"). For more information, see SCHNEIER, Bruce. Lessons from the Dyn DDoS Attack. Available at: [https://www.schneier.com/blog/archives/2016/11/lessons\\_from\\_th\\_5.html](https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html).
121. <sup>cxxi</sup>As reference, a list of products with compulsory certification by INMETRO appears in <http://www.inmetro.gov.br/qualidade/rtepac/compulsorios.asp>. There are already plans for evaluation of IoT devices by INMETRO. The Internal Regulation of the entity establishes that the Laboratory of Informatics is to develop software evaluation programs for the Internet of Things. Ordinance No. 2 of January 4, 2017 of the Ministry of Development, Industry and Foreign Trade (Internal Regulation of INMETRO), art. 84, available at [https://www.diariodasleis.com.br/legislacao/federal/exibe\\_artigo.php?ifl=235081](https://www.diariodasleis.com.br/legislacao/federal/exibe_artigo.php?ifl=235081).
122. <sup>cxxii</sup>ANATEL Resolution 242, November 30, 2000, (Regulamento para Certificação e Homologação de Produtos para Telecomunicações), available at <http://www.anatel.gov.br/legislacao/resolucoes/15-2000/129-resolucao-242>.
123. <sup>cxxiii</sup>Online Trust Alliance, 2017. Available at: [https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework6-22.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf).
124. <sup>cxxiv</sup>It should also be noted, according to a book published by the European Network and Information Security Agency, that the most common models for sharing information in countries of the European Union and the European Economic Area involve self- and co-regulation, rather than specific legislation. See European Union Agency for Network and Information Security (ENISA), 2015, Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, p. 6.
125. <sup>cxxv</sup>This is the model implemented in Germany, with the Cyber-Security Council, created in 2012. The German agency features participation from cybersecurity and public policy experts, in addition to members from the private sector, among them medium-sized and large companies and operators of critical infrastructure. The Board is composed of an Executive Committee, President and Vice-President. More information at <http://www.cybersicherheitsrat.de/english/about-us/>.
126. <sup>cxxvi</sup>HATMANN, I. A. A Autorregulação pelo Código: Características, Impacto e Limites de um Novo Modelo. In: LEAL, F. (coord.) Direito privado em perspectiva: teoria, dogmática e economia – São Paulo: Malheiros, 2016.
127. <sup>cxxvii</sup>BIHR, P 2017, *Trustmarks for IoT: ThingsCon Report*, commissioned by the Mozilla Foundation Open IoT Studio.
128. <sup>cxxviii</sup>Available at <https://www.ncsc.gov.uk/articles/become-cesg-approved-test-facility>.
129. <sup>cxxix</sup>CERT.br is the agency responsible for acting as a center for the treatment of information security incidents within the scope of the Brazilian Network Information Center ("NIC.br"). The agency also

---

publishes books and periodicals, with the aim of promoting awareness of the importance of cybernetic protection and training.

130. <sup>xxx</sup>Online Trust Alliance, 2017. Available at [https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework6-22.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf).
131. <sup>xxxi</sup>According to the *Impact Assessment* of the Proposal of a Regulation for Parliament and the European Council on ENISA, of 2017 and available at [http://eur-lex.europa.eu/resource.html?uri=cellar:2413e286-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC\\_2&format=PDF](http://eur-lex.europa.eu/resource.html?uri=cellar:2413e286-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF), p. 24. The Common Criteria is recognized by national certification bodies of the signatory countries of the international instrument the Common Criteria Recognition Arrangement (“CCRA”).
132. <sup>xxxi</sup>DigitalEurope, “DigitalEurope’s views on Cybersecurity Certification and Labelling Schemes”, 2017, available at [http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core\\_Download&EntryId=2365&language=en-US&PortalId=0&TabId=353](http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2365&language=en-US&PortalId=0&TabId=353).
133. <sup>xxxi</sup>The Trusted-IoT Label is not linked to international recognition mechanisms of the European Union, as a Common Criteria or SOG-IS mechanism. For more information, see European Commission, “Digital Single Market – Digitising European Industry Questions and Answers”, available at [http://europa.eu/rapid/press-release\\_MEMO-16-1409\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm).
134. <sup>xxxi</sup>The Online Trust Alliance has easy-to-access guidelines and checklists, through the website <https://otalliance.org/HonorRoll>. The entity’s activities are described in detail in the book “2017 Online Trust Audit & Honor Roll”, available at <https://otalliance.org/system/files/files/initiative/documents/2017trustaudit.pdf>.
135. <sup>xxxi</sup>The base text developed by #*iotmark*, and notes and commentary from participants is available at: [https://docs.google.com/document/d/1b\\_0Wz6pEM8282t8H4MMfBpfCBkxwNGYR1enJOTuolj4/edit#](https://docs.google.com/document/d/1b_0Wz6pEM8282t8H4MMfBpfCBkxwNGYR1enJOTuolj4/edit#). The text establishes five pillars for device security assessment: (i) systems backend (e.g., cryptography, attack resiliency, procedures for software update and device configuration); (ii) robustness for password definition; (iii) device specifications (e.g., firmware types and cryptographic mechanisms used, security setup and data control); (iv) additional specifications (e.g., hardware security options, resilience to local attacks); (v) commercial specifications (e.g., clear identification of means of contact and device lifecycle, privacy policy, compliance with local legislation on personal data protection, penetration testing, open source usage warning). Available at <https://iotmark.wordpress.com/security/>.
136. <sup>xxxi</sup>Available at [http://www2.inmetro.gov.br/pbe/pdf/folder\\_pbe.pdf](http://www2.inmetro.gov.br/pbe/pdf/folder_pbe.pdf).
137. <sup>xxxi</sup>Available in Bihr, P 2017, *Trustmarks for IoT: ThingsCon Report*, commissioned by the Mozilla Foundation’s Open IoT Studio, p. 67 – 71, 76.
138. <sup>xxxi</sup>Available at <https://www.thedigitalstandard.org/the-standard>.
139. <sup>xxxi</sup>There exist well-established models of infra- and inter-sectoral information sharing programs. As an example of infra-sectoral models, we cite specific energy programs (Distributed Energy Security Knowledge – DENSEK), public transportation (Transport Sector Information Exchange – TSIE), health (Zorg ISAC), banking and financial services (European Financial Institutes – Information Sharing and Analysis Centre) and promotion of Internet access (UK Network Security Information Exchange). On the other hand, inter-sector models were implemented in several countries, such as the United Kingdom (Cyber Security Coalition), Austria (The Austrian Trust Circle), Germany (Cyber Threat Intelligence Sharing Research Project) and in the European Union (Network and Information Security Platform and the European Advanced Cyber Defense Centre).
140. <sup>cd</sup>According to Ordinance No. 2/2008 of the GSI/PR, critical infrastructure is those facilities, services and goods that, if interrupted or destroyed, will have a serious social, economic, political, international or national security impact. Among these, the critical priority infrastructure are the energy, water, transportation, telecommunications and financial areas. Available at: <http://contadores.cnt.br/legislacoes/portaria-gsipr-no-2-de-8-de-fevereiro-de-2008.html>.

- 
141. <sup>cxli</sup> Available at [http://www.planalto.gov.br/ccivil\\_03/ Ato2007-2010/2009/Decreto/D7009.htm](http://www.planalto.gov.br/ccivil_03/ Ato2007-2010/2009/Decreto/D7009.htm).
142. <sup>cxlii</sup> Available at [http://dsic.planalto.gov.br/documentos/publicacoes/2\\_Guia\\_SICL.pdf](http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICL.pdf).
143. <sup>cxliiii</sup> For context on issues related to security in the electric sector, see FORMIGONI FILHO, José Reinaldo. Cibersegurança no Setor Elétrico: Ações internacionais e proposta para mitigar o problema no Brasil, 2016. Available at <https://pt.slideshare.net/JoseynaldoFormigoniF/cibersegurana-setor-eltrico-brasileiro-utcal-summit-2016-v3>.
144. <sup>cxliv</sup> For a broad vision of the vulnerabilities involved in the electric energy sector, see ANTUNES SOUZA, P. BRANQUINHO, M., KIEFER, SANTOS, C., VIDEIRA, E. Cyber Security para Sistemas de Automação de Energia – Como a Defesa em Profundidade Pode Aumentar a Segurança Cibernética em Instalações Críticas, available at <https://w3.siemens.com.br/home/br/automacao-energia/artigo-tec/Documents/Cyber-Security.pdf>.
145. <sup>cxlv</sup> MANNING, J, Factom receives second DHS grant for blockchain IoT project. Available at <https://www.ethnews.com/factom-receives-second-dhs-grant-for-blockchain-iot-project>. Accessed on September 27, 2017.
146. <sup>cxlvi</sup> SIGNORINI, M et al. Towards an internet of trust: issues and solutions for identification and authentication in the internet of things. 2015. Available at: <http://www.tdx.cat/bitstream/handle/10803/350029/tms.pdf?sequence=1>. Accessed October 1, 2017.
147. <sup>cxlvii</sup> GIPP, B; KOSTI, J; BREITINGER, C. Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain. MCIS. 2016. p. 51. Available at <http://aisel.aisnet.org/mcis2016/51/>. Accessed on October 3, 2017.
148. <sup>cxlviii</sup> Department of Homeland Security, DHS S&T Awards \$199K to Austin Based Factom Inc. for Internet of Things Systems Security. Available at: <https://www.dhs.gov/science-and-technology/news/2016/06/17/st-awards-199k-austin-based-factom-inc-iot-systems-security>. Accessed on September 28, 2017.
149. <sup>cxlix</sup> REESE, A. DoE Selects Guardtime to Develop Blockchain-Based Cybersecurity for Energy Grids. Available at <https://www.ethnews.com/doe-selects-guardtime-to-develop-blockchain-based-cybersecurity-for-energy-grids>. Accessed on September 28, 2017.
150. <sup>cl</sup> Available at: <http://www.ciab.org.br/publicacoes/edicao/69/ciab-febraban-apresenta-testes-com-blockchain>
151. <sup>cli</sup> CPqD, Blockchain Whitepaper, 2017. Available at <https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf>. Accessed on September 27, 2017.
152. <sup>clii</sup> The model allows a digital certification alternative to the one adopted by ICP-Brazil. Other entities may issue their own certification models, other than the ICP-Brazil standard, which will produce legal effects once accepted by the parties involved. This alternative is of limited effectiveness, since it only affects the parties within the relationship.
153. <sup>cliii</sup> For a general overview, see LEMOS, R. ‘Certificação digital é futuro de serviços públicos, mas ainda é cara no Brasil’. Available at: [www1.folha.uol.com.br/colunas/ronaldolemos/2017/07/1899775-certificacao-digital-e-futuro-de-servicos-publicos-mas-ainda-e-cara-no-brasil.shtml](http://www1.folha.uol.com.br/colunas/ronaldolemos/2017/07/1899775-certificacao-digital-e-futuro-de-servicos-publicos-mas-ainda-e-cara-no-brasil.shtml). Accessed on October 2, 2017.
154. <sup>cliv</sup> For an overview of the benefits of blockchain authentication, to the detriment of the unified method of public key infrastructure, see “Can Blockchain Save the Internet of Things?”. Available at <https://securityledger.com/2016/04/can-blockchain-save-the-internet-of-things/>. Accessed on September 28, 2017. For an analysis of costs of IoT device certification in blockchain, see BALDI, M et al. ‘Certificate Validation Through Public Ledgers and Blockchains’. ITASEC. 2017. p. 156-165, available at <http://ceur-ws.org/Vol-1816/paper-16.pdf>. Accessed on October 2, 2017.

- 
155. <sup>clv</sup>Law no. 12.965/2014, art. 9.
156. <sup>clvi</sup>Final opinion of the Special Committee in delivering an opinion to Bill No. 5.403, of 2001, p. 40, available at [www.camara.leg.br/internet/agencia/pdf/PL5403ParecerFinal.doc](http://www.camara.leg.br/internet/agencia/pdf/PL5403ParecerFinal.doc).
157. <sup>clvii</sup>Here we can mention the new Low Power Wide Area Networks (LPWA), which have gained prominence in the provision of connectivity to IoT, and which are not intended to provide connection to the public internet, due to its design focused on applications with very limited data rate, availability and quality of service. As an example, we have the SIGFOX network, operator in Brazil through the company WND Brasil, which according to Directive Release 1706/2017/SEI/ORLE/SOR-ANATEL will provide service to a specific group of users, which is characterized as Limited Private Service – LPS.
158. <sup>clviii</sup>This exception, which is already expressly established in the regulation of the Internet Framework for the Internet, was recommended in November 2017 by the Indian telecommunications authority (TRAI) to be part of the local regulation on the subject, precisely to enable the development of the Internet of Things in India [http://www.trai.gov.in/sites/default/files/Recommendations\\_NN\\_2017\\_11\\_28.pdf](http://www.trai.gov.in/sites/default/files/Recommendations_NN_2017_11_28.pdf)
159. <sup>clix</sup>According to the World Urbanization Prospects report, published by the United Nations in 2014. Available at: <https://esa.un.org/unpd/wup/publications/files/wup2014-highlights.Pdf>. Accessed on 10.09.2017.
160. <sup>clx</sup>According to the *Mapping Smart Cities in the EU* report, published by the European Parliament in 2014. Available at: [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE\\_ET\(2014\)507480\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf). Accessed on 10.09.2017.
161. <sup>clxi</sup>According to the *Mapping Smart Cities in the EU* report “the concept of a Smart City can be viewed as recognizing the growing and indeed critical importance of technologies (especially ICT) for improving a city’s competitiveness, as well as ensuring a more sustainable future, across networks of people, businesses, technologies, infrastructures, consumption, energy and spaces” (p. 23).
162. <sup>clxii</sup>For an analysis of the interconnection between the concept of smart cities and urban public policies, see: FERRAZ, Fábio. *As cidades inteligentes devem ser reflexo de uma sociedade inteligente* Nexo, Aug. 22, 2017. Available at: [https://www.nexojornal.com.br/ensaio/2017/As-cidades-inteligentes-devem-ser-reflexo-de-uma-sociedade-inteligente?utm\\_campaign=a\\_nexo\\_2017823&utm\\_medium=email&utm\\_source=RD+Station](https://www.nexojornal.com.br/ensaio/2017/As-cidades-inteligentes-devem-ser-reflexo-de-uma-sociedade-inteligente?utm_campaign=a_nexo_2017823&utm_medium=email&utm_source=RD+Station). Accessed on 10.09.2017.
163. <sup>clxiii</sup>Considering this chapter’s scope, consisting of analysis of the regulatory environment for cities to implement or foster the development of local IoT solutions, analysis will focus on public initiatives or cooperation between government and private initiative. However, one must keep in mind that IoT solutions are often designed and implemented exclusively by private agents.
164. <sup>clxiv</sup>The *Mapping Smart Cities in the EU* report (p. 24), argues that a smart city is not guided by central command from government computers that will try to predict and guide citizens’ decisions. Truly smart cities will consider their citizens’ contributions, and may find new ways to connect and understand collected data and information.
165. <sup>clxv</sup>A study developed in the United States shows ways in which federal data is relevant for the development of municipal public policies: <https://sunlightfoundation.com/cities-need-federal-data/>. Accessed on 11.14.2017.
166. <sup>clxvi</sup>The relevance of private initiative in the design and implementation of IoT solutions in Smart Cities is not ignored. The scope of the chapter is regulatory environment for city managers to implement and foster IoT solutions, so the focus is on solutions implemented directly by the public administration or in cooperation with private initiative.
167. <sup>clxvii</sup> According to Federal Decree no. 7.174/2010, those contracted must possess certifications issued by public or private institutions accredited by INMETRO, affirming the meeting of the following requirements, as provided by specific regulation: a) safety for the user and installations; b) electromagnetic

- 
- compatibility; c) power consumption. Beyond this, Inter-ministerial Ordinance no. 141/2014 requires that private IT providers: a) adopt the standards defined in the e-PING architecture; b) use cryptography for classified information; c) use access control and identity management tools and; d) in case of IT services related to e-mail provision, prevention of group/mass messages and malware detection tools.
168. <sup>clxviii</sup>The Institutional Security Cabinet of Presidency of the Republic has published to date 22 Complementary Norms on topics related to information security in the Federal Public Administration.
169. <sup>clxix</sup>Federal Decree no. 8.135/2013 does not clearly define IT services classified as “data communication”, indicating a broad interpretation of the concept. Inter-ministerial Ordinance no. 141/2014, which regulated the Decree, indicated, in a non-exhaustive way the services of; I – electronic mail; II – file sharing and synchronization; III – instant messaging; IV – conference (teleconference, telepresence and web conference); and V – voice communication over Internet protocol (VoIP).
170. <sup>clxx</sup>Requirement established by Federal Decree no. 8.135/2013. This rule has as exception the hypothesis predicted in article 7 of Inter-ministerial Ordinance no. 141/2014, applicable to cases in which there is no offer of service provision by supplying public bodies or entities.
171. <sup>clxxi</sup>PM Ordinance no. 20/2016 and Complementary Norm no. 14/IN01/DSIC/GSIPR. We also list Judgement no. 1.739/2015 of the Federal Court of Audit that analyses the panorama of hiring cloud computing services in the Federal Public Administration and presents recommendations of good practices.
172. <sup>clxxii</sup>As provided for in item 8 of “Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem” issued by the Ministry of Planning; In accordance with CN14/IN01/DSIC/GSIPR, bodies must require that, in contracting, data and information of those contracted must remain exclusively in national territory, including security copies (backups), to ensure all guarantees provided for by Brazilian law to both the contractor and the party responsible for storage of information in the cloud.
173. <sup>clxxiii</sup>“Drone” is the colloquial expression commonly used to designate “Remotely Piloted Aircraft”. The technical bodies use the abbreviation of the designation in English as a technical term to denominate drones: RPA. The most complete and adequate technical designation for the entire complex (aircraft - RPA, Remote Pilot Station, pilot engagement and any other component of the project) is “Remotely Piloted Aircraft System” (RPAS).
174. <sup>clxxiv</sup>Regulation related to the registry, use and inspection of drones is further detailed in the chapter on the rural environment.
175. <sup>clxxv</sup>Available at: <http://www.anatel.gov.br/institucional/ultimas-noticiass/2-uncategorised/1485-drones-devem-ser-homologados-para-evitar-interferencias>
176. <sup>clxxvi</sup>Brazilian Civil Aviation Special Regulation – RBAC-E n° 94 (RBAC-E n° 94). Available at: [http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00/@/@display-file/arquivo\\_norma/RBACE94EMD00.pdf](http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00/@/@display-file/arquivo_norma/RBACE94EMD00.pdf). Accessed on 10.01.2017.
177. <sup>clxxvii</sup>DECEA is the Aeronautical Command Agency with competence to “plan, manage and control activities related to airspace control, flight protection, search and rescue services and telecommunications of the Aeronautics Command.” Available at: <http://www.decea.gov.br/drone/>. The following regulations are applicable: Aeronautics Command Instruction (“ICA”) 100-40; Aeronautical Information Newsletter (“AIC”) - N 17, AIC-N 23 e AIC-N 24.
178. <sup>clxxviii</sup>This distance may be flexible before authorization of the owner of the building or installation.
179. <sup>clxxix</sup>Exception valid for cases in which there is a sufficiently strong barrier to protect and isolate people who are not involved in the operation from accidents.
180. <sup>clxxx</sup>This does not apply to the Public Power.
181. <sup>clxxxii</sup>Exception for drones owned by entities controlled by the State.



- 
182. <sup>clxxxii</sup>The prohibition of autonomous operations does not imply a prohibition of completely automated flights, which can occur as long as it is possible to intervene in the remote pilot, at any moment.
183. <sup>clxxxiii</sup> DECEA's institutional website has a simple example of how important it is for drone operators to observe rules for airspace use: The drone operator wants to perform a flight over an uninhabited area of up to 400ft AGL (approximately 120 meters high). ICA 100-4, which deals with helicopter operations, determines that the minimum height for helicopter flights over uninhabited areas is of 200ft (approximately 60 meters). From this example alone, it is easy to see that uncoordinated drone flights can cause conflict in helicopter traffic in the flight area, putting the helicopter at risk. Available at: <http://www.decea.gov.br/drone/>. Accessed on 10.01.2017.
184. <sup>clxxxiv</sup>Non-compliance with drone regulation in cities may cause considerable problems, such as the suspended airport activities a given period. In November 2017, Congonhas Airport in São Paulo suspended landings for two hours, causing the delay of numerous flights. See: <https://oglobo.globo.com/brasil/falta-de-fiscalizacao-sobre-drones-coloca-em-risco-seguranca-de-avioes-dizem-especialistas-22067331> Accessed on 01.30..2018
185. <sup>clxxxv</sup>Among those responsible for inspecting the use of drones are ANAC, DECEA, ANATEL and the public safety organs. However, this inspection has been facing issues due to (i) difficulty of individualizing the drone in an irregular situation and identifying its owner; or (ii) lack of staff to implement the necessary practices to identify wrongdoing.
186. <sup>clxxxvi</sup>This publication does not aim to evaluate the merit and results of the referenced projects. The scope is to analyze the regulatory environment for the implementation of IoT in cities, so our references to projects completed or underway is exclusively for illustrative purposes.
187. <sup>clxxxvii</sup>According to art. 14, I, of Decree no. 8.771, of 2016, personal data is defined as: “data related to an identified or identifiable individual, including identification numbers, locational data or electronic identifiers, when these are related to a person”.
188. <sup>clxxxviii</sup>Depending on topic developments, jurisprudence has also adopted provisions from the Consumer Defense Code, especially in cases of sharing registration databases without previous consent.
189. <sup>clxxxix</sup>A primary distinction between “public” and “private” spaces is necessary. For the purposes of this analysis, a public space is considered as a place that can be accessed by anyone, at any time and under any circumstance.
190. <sup>cx</sup>The concept of privacy as the individual control over their own personal data is fundamental to establish the right of self-determination in the context of personal data protection.
191. <sup>cxci</sup>The Constitution Project, Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties. p. 24. Available at: [https://www.law.berkeley.edu/files/Video\\_surveillance\\_guidelines.pdf](https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf). Accessed on 10.16.2017.
192. <sup>cxcii</sup>For broader analysis on doctrinal and seminal cases in the jurisprudence regarding expectation of privacy in public environments, see MOREHAM, N.A., Privacy in Public Places, 65 Cambridge Law Journal, 2006, p. 606-635.
193. <sup>cxciir</sup>The concern in these cases is that the collected data must be used only for the finality of its purpose. For example, the Public Power may collect necessary personal data to manage an electronic ticketing system (such as the “Bilhete Único” system in the city of São Paulo) for municipal public transportation. Considering that this data is essential to offer good service, consent is dismissed. However, the data must only be used for the specific finality of managing the service and must be stored with high levels of security and cannot be handed to third parties unrelated to the management of the service. Other data that might be collected and is not necessary for the service provision must be subjected to previous, free and informed consent by its subjects.
194. <sup>cxciiv</sup>The model is also implemented by jurisdictions like Uruguay. According to guidebook “Manejo de datos personales em la Administración Pública”, the handling of data by the Public Administration without

- previous consent from the data subject is allowed when (i) processing is necessary to provide “State duties”, and (ii) when personal data is collected through an anonymization process without identification of the subject. Available at: [http://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/e23f0f93-1004-4b65-833f-d1f74c347756/guia-4-web.pdf?MOD=AJPERES&CONVERT\\_TO=url&CACHEID=e23f0f93-1004-4b65-833f-d1f74c347756](http://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/e23f0f93-1004-4b65-833f-d1f74c347756/guia-4-web.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=e23f0f93-1004-4b65-833f-d1f74c347756). Accessed on 09.26.2017.
195. <sup>cxv</sup>The European Parliament and Council, Regulation (EU) 2016/679 of April 27, 2016. Available at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Accessed on 09.27.2017.
196. <sup>cxvi</sup>Project City Camera, in São Paulo, with the goal of installing and conducting urban monitoring through more than 10,000 surveillance cameras. Available at: <https://www.citycameras.prefeitura.sp.gov.br/howworks>. Accessed on 08.22.2017.
197. <sup>cxvii</sup>In Rio de Janeiro, the Command and Control Integrated Center (“CICC”) has access to the transmission of more than 3,000 surveillance cameras, used for public security. Available at: <https://goo.gl/zpTeRc> e <http://www1.folha.uol.com.br/cotidiano/2013/05/1277131-bbb-da-favela-da-rocinha-monitora-moradores-24-horas.shtml> MARTINEZ-BALLESTÉ, Antoni; PÉREZ-MARTINEZ, Pablo; SOLANAS, Agosti. The Pursuit of Citizens’ Privacy: a Privacy-Aware Smart City is Possible. Available at: <https://crises-deim.urv.cat/web/docs/publications/journals/794.pdf>. Accessed on 08.22.2017. Rio de Janeiro has a history of partnerships with big data companies. During the Olympic Games, the city hired telephone companies such as TIM to provide location data to its clients. Available at: <http://www.inova.jor.br/2016/07/22/tim-big-data/>. Accessed on 08.22.2017.
198. <sup>cxviii</sup>This suggestion reflects the mechanism adopted for national defense and public security in Uruguay. Law no. 18,331 of August 18 of 2008 establishes that the handling of data for these purposes by the armed forces, police or intelligence bodies is allowed even if without consent of the data subject, if in strict compliance with the object. Available at: [http://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/f085d1b8-0a24-4070-9dad-adc87b7595f2/18.331\\_con\\_modificaciones\\_de\\_la\\_19.355\\_.pdf?MOD=AJPERES&CONVERT\\_TO=url&CACHEID=f085d1b8-0a24-4070-9dad-adc87b7595f2](http://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/f085d1b8-0a24-4070-9dad-adc87b7595f2/18.331_con_modificaciones_de_la_19.355_.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=f085d1b8-0a24-4070-9dad-adc87b7595f2). Accessed on 09.26.2017.
199. <sup>cxix</sup>Smart Santander, Evaluation report on potentials of IoT for enhancing city services, 2014. Available at: [http://www.smartsantander.eu/downloads/Deliverables/D4.3\\_%20Final\\_version.pdf](http://www.smartsantander.eu/downloads/Deliverables/D4.3_%20Final_version.pdf). [https://www.fed4fire.eu/fileadmin/documents/public\\_deliverables/D4-3\\_Report\\_on\\_first\\_cycle\\_developments\\_of\\_the\\_services\\_and\\_applications\\_communityFed4FIRE\\_318389.pdf](https://www.fed4fire.eu/fileadmin/documents/public_deliverables/D4-3_Report_on_first_cycle_developments_of_the_services_and_applications_communityFed4FIRE_318389.pdf). Accessed on 09.25.2017.
200. <sup>cx</sup>It should be noted that Law no. 4,060/2012 has less stringent criteria for sensitive personal data collection in comparison to Bills no. 5,276/2016 and no. 330/2013. It does not consider genetic or biometric data as sensitive data, in addition to not addressing the criteria that classify valid consent.
201. <sup>cx</sup>KOSINSKI, Michal. WANG, Yilun. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images, *Journal of Personality and Social Psychology*. Available at <https://osf.io/zn79k/>. Accessed on 08.29.2017.
202. <sup>cxii</sup>In these cases, the principle of purpose is also essential. Facial data may be collected for the purpose of public security, but it may never be handled to analyze the data subject’s sexual orientation, which would be unnecessary, disproportionate and, just as importantly, goes beyond the purpose that justifies the data collection.
203. <sup>cxiii</sup>As a reference to cryptography mechanisms, the following are worth mentioning <https://cartilha.cert.br/criptografia/> and <https://cartilha.cert.br/mecanismos/>. Accessed on 08.29.2017.
204. <sup>cxiv</sup>It is the exclusive role of the Union to preside over matters referring to civil rights (article 22, I, Federal Constitution), including data protection. Any municipal law on data protection must handle only “subjects of local interest” (article 30, I, Federal Constitution), as a supplement to the federal legal framework, in order to avoid unconstitutionality due to a lack of competence. Municipal law must therefore address matters within the institutional or functional scope of the Municipal Administration.



---

For an overview on the concept of “local interest”, see: SILVA, José Afonso da. Comentário Contextual à Constituição, 9ª ed., São Paulo: ed. Malheiros, p. 314-315.

205. <sup>ccv</sup>This deals with, for example, the model adopted by the Wi-Fi solution (LinkNYC) in the city of New York, USA. City Hall disclosed a Privacy Policy on a website dedicated to the solution, with the description of data collection, use, storage and exclusion practices. Available at <https://www.link.nyc/privacy-policy.html>. Accessed on 08.22.2017.
206. <sup>ccvi</sup>PACHECO DA SILVA, A., CAMELO, A., LIGUORI FILHO, C., *et al*, *Um novo mundo de dados – relatório final*, (A new world of data – final report) GEPI – Grupo de Estudos em Pesquisa e Inovação (FGV), 2017, p. 38 - 40.
207. <sup>ccvii</sup>It may be the case of use of personal data for forensic investigation or commercial ends by the Public Power, for example.
208. <sup>ccviii</sup>The concepts of differential privacy and anonymization are addressed in detail in the sub-topic “Storage of personal data”.
209. <sup>ccix</sup>NEWCOMBE, Tod. Santander: The smartest smart city. Available at: <http://www.governing.com/topics/urban/gov-santander-spain-smart-city.html>. Accessed on 08.22.2017.
210. <sup>ccx</sup>Estonia has a history of sensitive data storage using blockchain technology, a system that also represents an interesting alternative for protecting personal data. In this case, the country uses this mechanism to register medical information of its citizens in a safe way. Available at: <https://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers>. Accessed on 08.22.2017.
211. <sup>ccxi</sup>See Opinion no. 50/2014 on anonymization from the “Data Protection Working Group in Article 29” from the European Commission. Available at: <http://www.gdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf>, p. 18-19. Accessed on 09.27.2017.
212. <sup>ccxii</sup>When contracting cloud computer services, for example, the Federal Public Administrations uses clauses that require its partners to respect information security techniques. The Terms of Reference published on 05/16/2017 for the contracting of infrastructure as a service (IaaS) and platform as a service (PaaS): <http://www.participa.br/contratacao-de-servicos-de-computacao-em-nuvem/servicos-de-computacao-em-nuvem-consulta-publica/consulta-publica-termo-de-referencia/termo-de-referencia-servicos-de-computacao-em-nuvem>.
213. <sup>ccxiii</sup>PACHECO DA SILVA, A., CAMELO, A., LIGUORI FILHO, C., *et al*, *Um novo mundo de dados – relatório final*, GEPI – Grupo de Estudos em Pesquisa e Inovação (FGV), 2017, p. 46 - 47. According to item 7.2.1 in the Terms of Reference, a partner can only share information in generic ways, meaning without the identification of users related to the information, considered individually.
214. <sup>ccxiv</sup>Here it is worth mentioning the example of information provision by the WiFi service of New York’s City Hall, in the United States, which includes 10,000 access kiosks around the city. Although not an IoT solution, the service collects personal data such as registration information and navigation history of users. Program representatives claim the collected information can only be Accessed by the Police Department through a court order. See the Privacy Policy of the LinkNYC program at: <https://www.link.nyc/privacy-policy.html>. More information on the program and the possibilities of personal data access by police authorities at: <https://www.fastcompany.com/3057980/privacy-concerns-raised-about-new-york-citys-free-wi-fi>.
215. <sup>ccxv</sup>This measure is already used in certain areas of the Public Administration. As an example, the Institutional Security Cabinet (GSI) issued Normative no. 1 of June 13 of 2008, in which it outlines guidelines for information security, among which is the implementation of awareness programs and programs to train human resources in information and communication security (Article 3, IV).
216. <sup>ccxvi</sup>Available at <https://data.ny.gov>. Accessed on 09.27.2017.

- 
217. <sup>ccxvii</sup> Available at <https://www.link.nyc/privacy-policy.html>, item “Cameras”. Accessed on 09.27.2017.
218. <sup>ccxviii</sup> Cf. MARTINI, José Sidnei Colombo. A gestão da infraestrutura urbana na cidade do futuro: Energia elétrica. In CASTRO, Nivaldo de J. (Org.). *Visão 2030. Cenários, tendências e novos paradigmas do setor elétrico*. Rio de Janeiro: Babilônia Cultural Editorial, 2015, p. 23.
219. <sup>ccxix</sup> Cf. ANTUNES, Vitor Amuri. *Parcerias público-privadas para smart cities*. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 19.
220. <sup>ccxx</sup> As shown in the partial report Produto 8: Aprofundamento de Verticais - Cidade, of September of 2017.
221. <sup>ccxxi</sup> More information at: <http://gizmodo.uol.com.br/infografico-o-que-e-como-funciona-e-quais-os-beneficios-do-smart-grid/>; <https://www.cplf.com.br/energias-sustentaveis/sites-tematicos/smart-grid/Paginas/default.aspx>; and <http://www.cemig.com.br/pt-br/A-Cemig-e-o-Futuro/sustentabilidade/nossos-programas/Redes-Inteligentes/Paginas/as-redes-inteligentes.aspx>. Accessed on 09.11.2017.
222. <sup>ccxxii</sup> For an analysis on the use of communication technologies in smart meters, see partial report Produto 8: Aprofundamento de Verticais - Cidade, of September of 2017, p.19.
223. <sup>ccxxiii</sup> MONZONI, Mario; NICOLETTI, Mariana. A cidade para os cidadãos: Mobilidade, energia e agricultura urbana. Caderno FGV Projetos, jun./jul. 2014, year 9, no. 24, p. 63. Available at: [http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos\\_fgvprojetos\\_smart\\_cities\\_gwa\\_0.pdf](http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_gwa_0.pdf). Accessed on 09.05.017.
224. <sup>ccxxiv</sup> For example, the Ministry of Mines and Energy created in 2010 a work group to analyze and identify measures capable of fostering the implementation of related public policies. For more information, see: BANDEIRA, Fausto de Paula Menezes. *Redes de Energia Elétrica Inteligentes (Smart Grids)*. Congress Advisory Technical Note. April of 2012. Available at: [http://www2.camara.leg.br/a-camara/documentos-e-pesquisa/estudos-e-notas-tecnicas/areas-da-conle/tema16/2012\\_7872.pdf](http://www2.camara.leg.br/a-camara/documentos-e-pesquisa/estudos-e-notas-tecnicas/areas-da-conle/tema16/2012_7872.pdf). Accessed on 09.13.2017.
225. <sup>ccxxv</sup> To accompany the aforementioned Bills, see: <https://www25.senado.leg.br/web/atividade/materias/-/materia/104860>, <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=535991>, <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1805590>, <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1713431>. Accessed on 09.13.2017.
226. <sup>ccxxvi</sup> See the partial report Produto 8: Aprofundamento de Verticais - Cidade, of September of 2017.
227. <sup>ccxxvii</sup> As observed by the partial report Produto 8: Aprofundamento de Verticais - Cidade, of September of 2017.
228. <sup>ccxxviii</sup> According to the partial report Produto 8: Aprofundamento de Verticais - Cidade, September 2017.
229. <sup>ccxxix</sup> ROMEIRO, Diogo Lisboa. *Do bitcoin à geração distribuída - A revolução da blockchain rumo à descentralização*. Available at: <https://infopetro.wordpress.com/2017/05/10/do-bitcoin-a-geracao-distribuida-a-revolucao-da-blockchain-rumo-a-descentralizacao/>. Accessed on 09.13.2017.
230. <sup>ccxxx</sup> As will be addressed, ANEEL has already regulated it since 2012, through Resolution no. 482, which has installed electric power compensation system through micro or mini-generation. On the subject, see ADAMI, Mateus Piva; CAMARGO, Manuela; KRAFT, Amanda Moreira. *Geração distribuída: avanços encorajados pela ANEEL*. Jota, São Paulo, August 15, 2017. Available at: <https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017>. Accessed on 09.12.2017. Through Resolution no. 687/2015, ANEEL has made alterations in this model, among which are the expansion of allowed sources (including renewable ones); the re-definition of maximum generation limits; the provision of new models (condominiums); and the stipulation of a more simplified and computerized process.

- 
231. <sup>ccxxxi</sup>RIVERA, Ricardo et al. Redes elétricas inteligentes (smart grid): Oportunidade para adensamento produtivo e tecnológico local. Available at: [https://web.bndes.gov.br/bib/jspui/bitstream/1408/2927/1/RB%2040%20Redes%20el%C3%A9tricas%20inteligentes\\_P.pdf](https://web.bndes.gov.br/bib/jspui/bitstream/1408/2927/1/RB%2040%20Redes%20el%C3%A9tricas%20inteligentes_P.pdf). Accessed on 09.05.2017.
232. <sup>ccxxxii</sup>This possibility is also regulated by ANEEL Resolution no. 502/2012 and can be implemented by concessionaries starting January, 2018. The subject will be addressed in more detailed further on. See: <http://atarde.uol.com.br/economia/noticias/1894067-tarifa-branca-comeca-em-janeiro-de-2018-diz-aneel> Accessed on 09.13.2017.
233. <sup>ccxxxiii</sup>The issue of electronic pre-payment and post-payment of electric power is one of the most regulated subjects by ANEEL through Resolution no. 610/2014.
234. <sup>ccxxxiv</sup>According to Maria Tereza Vellano, director of planning, engineering and distribution works of AES Eletropaulo, the smart meter used in a smart grid costs R\$800, while the conventional one costs R\$ 70. More information at: <http://redesinteligentesbrasil.org.br/component/content/article/13-ultimas-noticias/57-rede-eletrica-inteligente-ajuda-a-reduzir-perdas-o-estado-de-s-paulo.html>. Accessed on 09.11.2017.
235. <sup>ccxxxv</sup>ADI 3.558, vote of Minister Cármen Lúcia, j. 3-17-2011, P, DJE 5-6-2011.
236. <sup>ccxxxvi</sup>For more information, see: <http://www2.aneel.gov.br/biblioteca/downloads/livros/caderno-tematico-descentralizacao.pdf>. Accessed on 09.08.2017.
237. <sup>ccxxxvii</sup>Some decentralized activities are inspections, support of the regulation of electricity services and installations and mediation of problems among market agents. For more information, see: <http://www.aneel.gov.br/descentralizacao-de-atividades>
238. <sup>ccxxxviii</sup>For example, see the cooperation agreement between ANEEL and Arsep. Available at: [http://www.aneel.gov.br/documents/656877/15015002/ARSESP\\_19.2011.pdf/cce6347d-9361-4f8b-8145-85ac51029364](http://www.aneel.gov.br/documents/656877/15015002/ARSESP_19.2011.pdf/cce6347d-9361-4f8b-8145-85ac51029364)
239. <sup>ccxxxix</sup>Considering the competencies provided for by Law no. 9.427/1996 and regulated by Decree no. 2.335/1997. The Resolution is a consequence of Public Hearings no. 08/2008 and no. 02/2009 and resulted in the complete revocation of many of the Agency's previous resolutions. Text available at: <http://www2.aneel.gov.br/cedoc/ren2010414.pdf>. Accessed on 09.05.2017.
240. <sup>ccxli</sup>See article 73 and following.
241. <sup>ccxlii</sup>Approval of meters is not the role of ANEEL, but of the National Institute of Metrology, Quality and Technology – INMETRO. See legislation at: <http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001931.pdf>. Accessed on 09.05.2017.
242. <sup>ccxliii</sup>See article 84 and the ones that follow.
243. <sup>ccxliv</sup>The proposal to regulate the minimum requirements for power meters was discussed at Public Consultation 43/2010 and collected contributions from society between October 1, 2010 and January 28, 2011, with a live session held in Brasília on January 26, 2011. At the end of this period, ANEEL received 212 contributions from 57 agents, with suggestions from consumers, distributors, industries, sector associations and other segments of society. During the live session, there were 19 manifestations with comments and contributions. See: [http://www2.aneel.gov.br/aplicacoes/noticias/Output\\_Noticias.cfm?Identidade=5903&id\\_area=90](http://www2.aneel.gov.br/aplicacoes/noticias/Output_Noticias.cfm?Identidade=5903&id_area=90). Accessed on 09.10.2017.
244. <sup>ccxlv</sup>Available at: <http://www2.aneel.gov.br/cedoc/ren2012502.pdf>. Accessed on 09.05.2017.
245. <sup>ccxlvi</sup>Available at: <http://www2.aneel.gov.br/cedoc/ren2016732.pdf>. Accessed on 09.08.2017.
246. <sup>ccxlvii</sup>See Article 1 of Resolution no. 502/2012.

- 
247. <sup>ccxlvii</sup>Source: <http://atarde.uol.com.br/economia/noticias/1894067-tarifa-branca-comeca-em-janeiro-de-2018-diz-aneel>. Accessed on 09.13.2017.
248. <sup>ccxlviii</sup>The option is an assurance for consumers who cannot change habits to consume less during peak hours.
249. <sup>ccxlix</sup>More information at: [http://www2.aneel.gov.br/aplicacoes/noticias/Output\\_Noticias.cfm?Identidade=5912&cid\\_area=90](http://www2.aneel.gov.br/aplicacoes/noticias/Output_Noticias.cfm?Identidade=5912&cid_area=90). Accessed on 09.05.2017.
250. <sup>cccl</sup>The first distributor to have smart meters authorized by INMETRO was AES Eletropaulo, in 2016, through Ordinances no. 586/2012, no. 587/2012 and no. 520/2014. More information at: <https://www.weg.net/institucional/BR/pt/news/produtos-e-solucoes/weg-tem-o-primeiro-medidor-de-energia-do-brasil-certificado-pelo-inmetro> and <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=43137&sid=3>. Accessed on 09.05.2017.
251. <sup>cccli</sup>Another example is Ecil Energia, a company that also had smart meters authorized by INMETRO in the past few years. More information at: <http://www.ecilenergia.com.br/download/Medidores.pdf>. Accessed on 09.11.2017.
252. <sup>ccclii</sup>It is necessary to evaluate the viability of and financial incentives for the substitution, especially since the form of compensation of concessionaires for investments considers the depreciation rate of the devices, calculated based on the age, useful life, state of maintenance, conservation and obsolescence (Annex V of Resolution no. 493/2002). With an updated technology park without devices that are close to obsolescence, the onus for the modernization of measuring devices will fall essentially on the concessionaires. Resolution at: <http://www2.aneel.gov.br/ccdoc/res2002493.pdf?%20Acesso%20em%2003.10.2017>. Accessed on 09.10.2017.
253. <sup>cccliii</sup>The proposal establishes that electricity concessionaires must adjust their distribution systems to implement all the necessary requirements for their transformation into Smart Grids (article 1). Among the guidelines for the implementation of the grids is the provision of measuring sensors, automation devices, a reliable communication system among all automation devices and the possibility of instantaneous and bi-directional transfer of information between devices (article 3).
254. <sup>cccliv</sup>Bill no. 3.337 provides in a more specific way that concessionaires must substitute all electromechanical power meters for electronic meters in the period of up to 10 years (article 1). It also regulates, in Articles 2 and 3, the commercialization of excess energy produced by consumers.
255. <sup>ccclv</sup>Bill no. 2.932 provides for the National Plan of Electric Smart Grids. Similar to the previous Bill, it determines concessionaires must substitute traditional meters for smart meters, however, within a more extensive period of up to 15 years from the publication of the law (Article 3). It also provides on the commercialization of excess energy (article 6). Bill no. 3.138 is also before Congress and has similar provisions.
256. <sup>ccclvi</sup>For more information on current meter regulations, see: [http://www.aneel.gov.br/documents/656827/14866914/Modulo5\\_Revisao5/4d9e298e-cbf6-4b09-a01a-2e55f05dc9c7](http://www.aneel.gov.br/documents/656827/14866914/Modulo5_Revisao5/4d9e298e-cbf6-4b09-a01a-2e55f05dc9c7). Accessed on 09.18.2017.
257. <sup>ccclvii</sup>Even if instrumentalization independent from the use of smart meters is possible, distributed generation may be enhanced by this technology. Low users can adhere to the policy of mini or micro-grid distributed generation with unidirectional meters. See: [http://www2.aneel.gov.br/arquivos/PDF/FAQ\\_GD\\_Atualizado.pdf](http://www2.aneel.gov.br/arquivos/PDF/FAQ_GD_Atualizado.pdf). Accessed on 09.13.2017.
258. <sup>ccclviii</sup>To charge consumer units in the compensation system, the contributed energy must be considered and subtracted from the consumed energy (Article 7).
259. <sup>ccclix</sup>Available at: <http://www2.aneel.gov.br/ccdoc/ren2015687.pdf>. Accessed on 09.14.2017.

- 
260. cclx After issuing the resolution, there has been more significant increase in program adoption. See: [http://www.aneel.gov.br/documents/656827/15234696/Nota+T%25C3%25A9cnica\\_0056\\_PROJE%25C3%2587%25C3%2595ES+GD+2017/38cad9ae-71f6-8788-0429-d097409a0ba9](http://www.aneel.gov.br/documents/656827/15234696/Nota+T%25C3%25A9cnica_0056_PROJE%25C3%2587%25C3%2595ES+GD+2017/38cad9ae-71f6-8788-0429-d097409a0ba9). Accessed on 09.14.2017.
261. cclxi ADAMI, Mateus Piva; CAMARGO, Manuela; KRAFT, Amanda Moreira. Geração distribuída: avanços encorajados pela ANEEL. Jota, São Paulo, August 15, 2017. Available at: <https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017>. Accessed on 09.12.2017.
262. cclxii Source: [https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017#\\_ftn2](https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017#_ftn2). Accessed on: 09.13.2017.
263. cclxiii See: [http://www.aneel.gov.br/documents/656827/15234696/Nota+T%25C3%25A9cnica\\_0056\\_PROJE%25C3%2587%25C3%2595ES+GD+2017/38cad9ae-71f6-8788-0429-d097409a0ba9](http://www.aneel.gov.br/documents/656827/15234696/Nota+T%25C3%25A9cnica_0056_PROJE%25C3%2587%25C3%2595ES+GD+2017/38cad9ae-71f6-8788-0429-d097409a0ba9) Accessed on 09.18.2017.
264. cclxiv This kind of movement is found in the recent Confaz Agreement 16/2015, which authorized the states of Goiás, Pernambuco and São Paulo to conceive ICMS exemption on electricity provided by distributors to consumer units through micro and mini-grids. In: FREITAS, Bruno M. R. e HOLLANDA, Lavinia. Micro e minigeração no Brasil: Viabilidade econômica e entraves do setor. *White Paper* n. 1, May 2015, Fundação Getúlio Vargas – FGV. Available at: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/13853/micro.pdf?sequence=1>. Accessed on 11.14.2017.
265. cclxv Source: <http://atarde.uol.com.br/economia/noticias/1894067-tarifa-branca-comeca-em-janeiro-de-2018-diz-aneel>. Accessed on 09.13.2017.
266. cclxvi See: [http://www.aneel.gov.br/sala-de-imprensa-exibicao/-/asset\\_publisher/XGPXSqdMFHrE/content/aneel-aprova-tarifa-branca-nova-opcao-para-os-consumidores-a-partir-de-2018/656877?inheritRedirect=false](http://www.aneel.gov.br/sala-de-imprensa-exibicao/-/asset_publisher/XGPXSqdMFHrE/content/aneel-aprova-tarifa-branca-nova-opcao-para-os-consumidores-a-partir-de-2018/656877?inheritRedirect=false) Accessed on 09.18.2017.
267. cclxvii See: <http://www2.aneel.gov.br/ccdoc/ren2014610.pdf> Accessed on 09.18.2017.
268. cclxviii For this reason, in this model, energy bills with consolidated information must be requested from the distributor by the consumer.
269. cclxix Supreme Court, 1st Panel, Resp 1270339/SC, Min. Rel. Gurgel de Faria, d.j. 12.15.2016. Available at: <https://enciclopediajuridica.pucsp.br/verbete/87/edicao-1/principio-da-continuidade-do-servico-publico-e-interruptao>. Accessed on 09.14.2017. The Court had already issued its uniform understanding of the lawfulness of suspended service for non-payment in 2003, in Resp 363.943/MG. Previous to this standardization, the 1st Panel contained interruption of essential services, while the 2nd Panel was inclined to permit such action. More in: SUZIN, Juliana Bonella. Suspensão do fornecimento de energia elétrica por inadimplemento. Available at: [http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2012\\_2/juliana\\_suzin.pdf](http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2012_2/juliana_suzin.pdf). Accessed on 09.14.2017.
270. cclxx According to the National Association of Energy Consumers, the implementation of the binomial tariff for low-voltage consumers could increase in up to 30% the return time of distributed generation projects. See: <http://www.anacebrasil.org.br/noticias/tarifa-binomia-aumentara-tempo-de-retorno-dos-projetos-de-gd/>. Accessed on 10.11.2017.
271. cclxxi For example, there have been reports of data on electricity consumption used by police authorities in the states of Texas and California to identify possible *cannabis* planting in residences and, consequently, to obtain search warrants. Source: Balancing access to electricity data and privacy concerns, PV Magazine, May 11, 2017. Available at: <https://pv-magazine-usa.com/2017/05/11/guest-column-balancing-access-to-electricity-data-and-privacy-concerns/>. Accessed on 09.14.2017.

- 
272. <sup>ccxxii</sup> As seen in the partial report Produto 8: Aprofundamento de Verticais - Cidade, of September 2017, information on instantaneous consumption may indicate if a residence is empty at the time, making it more susceptible to invasions.
273. <sup>ccxxiii</sup> List of practices published by the *Electronic Privacy Information Center*, available at: <https://epic.org/privacy/smartgrid/smartgrid.html>. Accessed on 09.18.2017.
274. <sup>ccxxiv</sup> GOODIN, Dan. Hackers lie in wait after penetrating US and Europe power grid networks. September 6, 2017. Available at: <https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/?comments=1>. Accessed on 09.18.2017. For example, in December 2015, an attack on the electricity distribution center near Kiev, in Ukraine, cut the power of about 225,000 people for six hours. This was the first hacking occurrence known for interrupting electricity on a large scale.
275. <sup>ccxxv</sup> VOLZ, Dustin. Hackers gain entry into U.S., European energy sector, Symantec warns. September 6, 2017. Available at: <http://www.reuters.com/article/us-usa-cyber-energy/hackers-gain-entry-into-u-s-european-energy-sector-symantec-warns-idUSKCN1BH171>. Accessed on 09.18.2017. ALEEM, Zeeshan. Russia-linked hackers are infiltrating the US power grid: report. September 6, 2017. Available at: <https://www.vox.com/world/2017/9/6/16262198/hackers-us-power-grid-russia>. Accessed on 09.18.2017.
276. <sup>ccxxvi</sup> Goodin observes that hackers in control of the operational system would be able to open the network to other invaders and also to hijack the system that monitors the quality of the network In: Hackers lie in wait after penetrating US and Europe power grid networks. September 6, 2017. Available at: <https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/?comments=1>. Accessed on 09.18.2017.
277. <sup>ccxxvii</sup> During the 2015 attack in Ukraine, passwords and other types of data were collected and allowed invaders to access the network's levels of supervision. In result, user data were unprotected and vulnerable to access. In: GOODIN, Dan. Hackers lie in wait after penetrating US and Europe power grid networks. September 6, 2017. Available at: <https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/?comments=1>. Accessed on 09.18.2017.
278. <sup>ccxxviii</sup> HERN, Alex. Smart electricity meters can be dangerously insecure, warns expert. December 29, 2016. Available at: <https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers>. Accessed on 09.18.2017.
279. <sup>ccxxix</sup> Source: <http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/>. Accessed on 09.18.2017.
280. <sup>ccxxx</sup> MARTINI, José Sidnei Colombo. A gestão da infraestrutura urbana na cidade do futuro: energia elétrica. In CASTRO, Nivaldo de J. (Org.). *Visão 2030. Cenários, tendências e novos paradigmas do setor elétrico*. Rio de Janeiro: Babilônia Cultural Editorial, 2015, p. 49-51.
281. <sup>ccxxxi</sup> More information at: <https://www.voltimum.pt/artigos/noticias-do-sector/smart-city-iluminacao-conectada-atraves-de-software-de-gestao-de-luz>. Accessed on 09.04.2017.
282. <sup>ccxxxii</sup> LED lights have a technology that enables the adjustment of brightness and intensity (from 0 to 100%) through a dimmer. The use of the dimmer increases the durability of the bulb and enables a drastic reduction in consumption. More information at: <http://www.g20brasil.com.br/o-conforto-e-a-economia-na-dimerizacao-com-bulbadas-de-led/>. Accessed on 08.04.2017.
283. <sup>ccxxxiii</sup> ANTUNES, Vitor Amuri. Parcerias público-privadas para cidades inteligentes. Available at: <http://www.pppbrasil.com.br/portal/content/artigo-parcerias-p%C3%BAblico-privadas-para-cidades-inteligentes?page=5>. Accessed on 08.24.2017.
284. <sup>ccxxxiv</sup> Smart lighting, connected to the Internet of Things, may work as a platform for a series of sensor technologies that collect data on traffic and people movement, public security, parking, air quality, climate, pollution, sound, seismic activity and others. More information at:



- 
- <http://www.archdaily.com.br/br/785682/iluminacao-conectada-da-ethernet-a-internet-li-fi> and <http://ofuturodascoisas.com/uma-iluminacao-publica-inteligente-e-que-gera-receita-para-cidade/>. Accessed on 09.04.2017.
285. <sup>ccxxxv</sup> Available at: <http://www.aneel.gov.br/documents/656877/14486448/bren2010414.pdf/3bd33297-26f9-4ddf-94c3-f01d76d6f14a?version=1.0>. Accessed on 08.15.2017.
286. <sup>ccxxxvi</sup> See the rapporteur's vote on the public hearing, available at: [http://www2.aneel.gov.br/aplicacoes/audiencia/arquivo/2013/107/resultado/voto\\_do\\_diretor\\_relator.pdf](http://www2.aneel.gov.br/aplicacoes/audiencia/arquivo/2013/107/resultado/voto_do_diretor_relator.pdf). Accessed on 08.15.2017.
287. <sup>ccxxxvii</sup> Available at: <http://www2.aneel.gov.br/cedoc/ren2013587.pdf>. Accessed on 08.15.2017.
288. <sup>ccxxxviii</sup> As a rule, most poles are an asset of the electricity sector, but there are situations in which they are installed by telecommunication companies or owned by the cities. We will address the second case, which seems to be the most complex and common.
289. <sup>ccxxxix</sup> See: <https://oglobo.globo.com/sociedade/tecnologia/operadoras-apostam-nas-antenas-em-postes-de-luz-para-melhorar-cobertura-9815112> Accessed on 09.19.2017.
290. <sup>ccxc</sup> Original Bill available at: <http://documentacao.camara.sp.gov.br/iah/fulltext/projeto/PL0751-2013.pdf> Accessed on 09.20.2017.
291. <sup>ccxci</sup> <http://www.telesintese.com.br/nova-proposta-de-lei-das-antenas-em-sao-paulo-reve-conceito-de-erb/> Accessed on 09.20.2017.
292. <sup>ccxcii</sup> This infrastructure sharing allows the enhancement of the already existing structure, reduction of costs for pole installation and maintenance and may at times make possible the expansion of the structure for which installation would not be viable on an individual basis. SUNDFELD, Carlos Ari. Estudo Jurídico sobre o preço de compartilhamento de infraestrutura de energia elétrica. Revista Eletrônica de Direito Administrativo Econômico, no. 4, November/December of 2006. Available at: <http://www.direitodoestado.com/revista/REDAE-4-NOVEMBRO-2005-CARLOS%20ARI%20SUNDFELD.pdf> Accessed on 09.19.2017.
293. <sup>ccxciii</sup> ANP also signs because the Resolution also concerns pipelines.
294. <sup>ccxciv</sup> Result of ANATEL Public Consultation no. 30/2013 and ANEEL Public Hearing no. 07/2007.
295. <sup>ccxcv</sup> See, for example: <https://www.aesetropaulo.com.br/padroes-e-normas-tecnicas/manuais-normas-tecnicas-e-de-seguranca/Documents/Padr%C3%B5es%20e%20Normas%20T%C3%A9cnicas/ID-4.044-Compartilhamento%20de%20Infraestrutura%20de%20RDA%20com%20Redes%20de%20Telecomunica%C3%A7%C3%B5es.pdf>, [http://www.celesc.com.br/portal/images/arquivos/normas/AnexoII-13130015-Compartilhamento\\_Postes-23-11-09.pdf](http://www.celesc.com.br/portal/images/arquivos/normas/AnexoII-13130015-Compartilhamento_Postes-23-11-09.pdf) and [http://www.eneldistribuicao.com.br/rj/documentos/PE2012\\_R-02.pdf](http://www.eneldistribuicao.com.br/rj/documentos/PE2012_R-02.pdf) Accessed on 09.20.2017
296. <sup>ccxcvi</sup> See: <http://www.abranet.org.br/Noticias/Provedores-alertam-que-acordo-Anatel%7CAneel-por-postes-nao-funciona-na-pratica-1515.html?UserActiveTemplate=site#.WcEoWrKGO01> Accessed on 09.19.2017.
297. <sup>ccxcvii</sup> In short, *ran sharing* is a type of sharing used by Brazilian operators, which may assume different models and allows the sharing of an access and frequency network by two or more telecommunication companies. The alternative has been greatly used by Brazilian telecom companies, as shown at: <http://www.telesintese.com.br/projeto-de-ran-sharing-entre-tim-oi-e-accenture-ganha-premio-em-barcelona/> However, the initiative has been questioned by tower owners, as the sharing would reduce their revenue, as the price of fixation points is currently charged per occupied space – and not per quantity of operators who effectively occupy the tower.
298. <sup>ccxcviii</sup> See, for example, the conflict between Nextel and SBA Torres related to the ran sharing contract established between Vivo and Nextel, addressed to ANATEL (ANATEL Process no. 53504.011048/2016-

- 
- 12, parties: NEXTEL TELECOMUNICAÇÕES LTDA., SBA TORRES BRASIL, judged on 12/21/2016).
299. <sup>cccix</sup>See: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2093587> Accessed on 09.19.2017.
300. <sup>ccc</sup>See: <http://economia.estadao.com.br/blogs/radar-imobiliario/nos-edificios-topo-e-subsolo-podem-ser-fontes-de-renda/> e <http://www.abc.com.br/noticias/economia/2013/12/operadoras-de-celular-buscam-alternativas-para-instalacao-de-antenas-e> Accessed on 09.21.2017
301. <sup>ccci</sup>See arguments and deliberations on the approval of Summary Statement no. 41, which determines that the service of public lighting cannot be remunerated by tariffs, available at: <http://www.stf.jus.br/portal/jurisprudencia/menuSumario.asp?sumula=2218> Accessed on 09.04.2017.
302. <sup>ccci</sup>ANTUNES, Vitor Amuri. Parcerias público-privadas para cidades inteligentes. Available at: <http://www.pppbrasil.com.br/portal/content/artigo-parcerias-p%C3%BAblico-privadas-para-cidades-inteligentes?page=5>.
303. <sup>ccciii</sup>In this context, see the opinion of the Special Commission on the proposed constitutional amendment PEC no. 559/2002 of the Federal Senate, available at: [http://www.camara.gov.br/proposicoesWeb/prop\\_mostrarintegra?codteor=85426&filename=PRL+1+PEC50402+%3D%3E+PEC+559/2002](http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=85426&filename=PRL+1+PEC50402+%3D%3E+PEC+559/2002) Accessed on: 09.04.2017.
304. <sup>ccciv</sup>Updates on the case may be accessed at: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=105304> Accessed on 09.04.2017.
305. <sup>ccciv</sup>The Parliamentary Front for Support of Smart and Human Cities proposes, among its priorities, the alteration of the COSIP law, allowing its resources to be used also in the installation of efficient and integrated technologies, directed at implementation of smart cities. More information at: <http://fpcidadesinteligentes.com.br/index.php/5-prioridades-iniciais/>. Accessed on 08.24.2017.
306. <sup>ccciv</sup>The improvement and expansion of the network involve activities such as project development, purchase of materials and equipment, and construction work.
307. <sup>cccvii</sup>In addition, the Federal Prosecutor (PGR) affirmed that ‘the inclusion of network improvement and expansion activities among the actions to be financed by the contribution is a necessary measure for the public lighting service to be provided in its full potential, since there is no better way than to contribute within the terms constitutionally established, to have the service provided with isonomy, efficiency and quality. Available at: <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4179476>. Accessed on: 08.24.2017.
308. <sup>cccvi</sup>Smart City Network proposal, available at: <http://fpcidadesinteligentes.com.br/index.php/5-prioridades-iniciais/>. Accessed on 09.04.2017.
309. <sup>cccix</sup>It is important to reinforce that other aspects of PPP regulation demand reflection and deepening. However, this report will only address matters related to the implementation of a smart public lighting network in the cities.
310. <sup>cccix</sup>ANTUNES, Vitor Amuri. Parcerias público-privadas para smart cities. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 40-41.
311. <sup>cccxi</sup>Cf. ANTUNES, Vitor Amuri. Parcerias público-privadas para smart cities. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 43.
312. <sup>cccxi</sup>Although the text in article 11 of Law no. 11.079/2004 determines that accessory funds must be destined to the promotion of tariff moderation, there are precedents in the Union Court of Audit that approve their use to promote the economic viability of a consideration contract of the government (Judgement 2886/2008, Judge Ubiratan Aguiar, j. 12.03.2008).



- 
313. <sup>cccxi</sup>In example, the development of LED bulbs with additional functions than the simple lighting of public spaces, collaborating to data supply for transportation services and public security, allowed the signing of partnership contracts that predict financial compensation to the concessionaire.
314. <sup>cccxiv</sup>Such revenues do not substitute for the use of COSIP and could be earned by the concessionaire as a consequence of providing services related to the object of the contract.
315. <sup>cccxv</sup>TUROLLA, Frederico; ALLAIN, Marcelo; ANKER, Thomas. Iluminação pública para cidades inteligentes. Valor Econômico. São Paulo, August 28 of 2014. Available at: <http://www.provedor.nuca.ie.ufrj.br/eletrobras/estudos/turolla1.pdf>. Accessed on 08.15.2017.
316. <sup>cccxvi</sup>ANTUNES, Vitor Amuri. Parcerias público-privadas para smart cities. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 48.
317. <sup>cccxvii</sup>Ibid., p. 51.
318. <sup>cccviii</sup>Inter-Municipal Public Lighting Consortium of Alagoas (Intermunicipal Consortium), Inter-Municipal Public Consortium of Agreste Pernambucano (Intermunicipal Consortium) and Complex Consortium Nascentes do Pantanal, in Maranhão (Consortium).
319. <sup>cccix</sup>Cf. ANTUNES, Vitor Amuri. Parcerias público-privadas para smart cities. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 52.
320. <sup>cccix</sup>Cf. ANTUNES, Vitor Amuri. Parcerias público-privadas para cidades inteligentes. Available at: <http://www.pppbrasil.com.br/portal/content/artigo-parcerias-p%C3%BAblico-privadas-para-cidades-inteligentes?page=5>.
321. <sup>cccxi</sup>Initially, the court stated the bid “could not proceed”. Later, it decided that, in order to proceed, “adjustments” would be needed. More information at: <http://g1.globo.com/sao-paulo/noticia/2015/10/tcm-autoriza-retomada-de-licitacao-da-ppp-da-iluminacao-publica-em-sp.html>; <https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2016/10/14/mais-uma-vez-justica-suspende-ppp-da-iluminacao-de-sao-paulo.htm>; and <http://g1.globo.com/sao-paulo/noticia/2016/10/gestao-haddad-retoma-ppp-da-iluminacao-publica.html>. Accessed on 08.24.2017.
322. <sup>cccxi</sup>See: <http://sao-paulo.estadao.com.br/noticias/geral,mais-uma-vez-justica-suspende-ppp-da-iluminacao-de-sp,10000082137> Accessed on 09.21.2017.
323. <sup>cccxi</sup>See: <http://www.pppbrasil.com.br/portal/content/tcm-suspende-sess%C3%A3o-de-abertura-de-propostas-comerciais-na-ppp-de-ilumina%C3%A7%C3%A3o-p%C3%BAblica-de-s%C3%A3o-> Accessed on 09.21.2017.
324. <sup>cccxiv</sup>The full statement and its modifications are available at: <http://www.prefeitura.sp.gov.br/cidade/secretarias/obras/ilume/noticias/?p=206645>
325. <sup>cccxv</sup>As in: <http://www.ul.com/inside-ul/street-smart-security-for-connected-lighting-infrastructure-2/>. Accessed on 09.20.2017. In Doncaster, United Kingdom, public lighting poles received 33,000 LED points that use wireless broadband technology to turn each bulb into a router. Source: <http://www.techradar.com/news/world-of-tech/why-you-should-be-worried-about-connected-street-lights-1327834>. Accessed on 09.20.2017.
326. <sup>cccxvi</sup>Details on equipment are available in the Security in Cities section.
327. <sup>cccxvii</sup>Through the implementation of surveillance devices of intense illumination, the city of Nice in France expects to reduce electricity costs by approximately eight million dollars. In: CHAMBERS, John; ELFRINK, Wim. The future of cities: The internet of everything will change how we live. Foreign Affairs. October 31, 2014. Available at: <https://www.foreignaffairs.com/articles/2014-10-31/future-cities>. Accessed on 09.20.2017.

- 
328. <sup>cccxxviii</sup>Source: <https://www.nytimes.com/2014/02/18/business/at-newark-airport-the-lights-are-on-and-theyre-watching-you.html>. Accessed on 09.20.2017.
329. <sup>cccxxix</sup>Source: <http://www.ul.com/inside-ul/street-smart-security-for-connected-lighting-infrastructure-2/>. Accessed on 09.20.2017.
330. <sup>cccxxx</sup>The company responsible for the Sensity Systems technology, directed to the installation of LED fixtures and sensors, declares its intention to address privacy issues related to its activities by acting in partnership with the American Civil Liberties Union (ACLU) and by implementing a post responsible for dealing with related matters (chief privacy officer). Declaration available at: <https://atelier.bnpparibas/en/smart-city/article/turning-street-lighting-system-gathering-big-data>. Accessed on 09.20.2017.
331. <sup>cccxxxI</sup>Listed in partial report Produto 8: Aprofundamento de Verticais - Cidade, of September 2017. In the same context, see: <http://sengeba.org.br/wp-content/uploads/2015/09/merged.pdf>. Accessed on 09.15.2017.
332. <sup>cccxxxii</sup>Acknowledging the work of Pedro do Carmo Baumgratz de Paula for his contributions on mobility related IoT. See his work on mobility and smart cities at: <http://sengeba.org.br/wp-content/uploads/2015/09/merged.pdf> and <http://www.ibdu.org.br/eficiente/sites/ibdu.org.br/pt-br/site.php?secao=noticias&pub=62>. Accessed on 11.14.2017.
333. <sup>cccxxxiii</sup>The Federal Supreme Court has reaffirmed its understanding of the Union’s exclusive competency to legislate on transit and transportation. In this sense, the Federal Supreme Court stated that the regulation of the introduction of electronic barriers to assess the speed of vehicles is an exclusive competency of the Union, as it is part of traffic (article 22, XI, of FC/1988). [ADI 2.718, Judge Joaquim Barbosa, j. 6-4-2005, P, DJ de 24-6-2005.] ADI 3.897, Judge Gilmar Mendes, j. 4-3-2009, P, DJE de 4-24-2009”. Also see ADI 3.671 MC, Judge Cezar Peluso, j. 8-28-2008, P, DJE de 11-28-2008.”
334. <sup>cccxxxiv</sup>The Federal Supreme Court stated that Article 1 of the Law of Santa Catarina includes matters related to the competency of the Union, the States, the Federal District and the Cities, as provided in item XII of article 23 of the FC, as it may determine obligations as long as they are relevant to the competencies of the State and related to public safety and traffic education (ADI 2.407, Judge Carmen Lúcia, j. 5-31-2007, P, DJ de 6-29-2007).
335. <sup>cccxxxv</sup>It is the responsibility of the Union to allow, through authorization, concession or permission, private entities to explore interstate road transportation services (article 21, XII, FC).
336. <sup>cccxxxvi</sup>The Federal Supreme Court ruled that “Member states are competent for exploring and regulating intermunicipal public transportation services (...) “The provision of urban transportation, characterized as a public service of local interest, is a subject of municipal legal competence, not applicable for member states to decide on (ADI 2.349, Judge Eros Grau, j. 8-31-2005, P, DJ de 10-14-2005).
337. <sup>cccxxxvii</sup>For a detailed analysis on the use of surveillance cameras by the Public Power, see contributions listed in the topic that addresses security in cities. We have described experimental advances tested by CCTV (closed circuit television) systems and how they can affect the privacy of citizens.
338. <sup>cccxxxviii</sup>In this context, the partial report Produto 8: Aprofundamento de Verticais - Cidade, of September 2017, points out that radars installed in strategic spots are used not only to control speed but also to identify all vehicles that pass by.
339. <sup>cccxxxix</sup>London has inaugurated a sidewalk capable of generating energy through the pressure created by pedestrian footsteps. See: <http://ciclovivo.com.br/noticia/rua-inteligente-que-gera-energia-e-inaugurada-em-londres/> and <http://www.techtudo.com.br/artigos/noticia/2011/03/conceito-uma-calcada-que-transforma-passos-de-pedestres-em-energia.html> Accessed on 11.14.2017.
340. <sup>cccxl</sup>As seen in the partial report Produto 8: Aprofundamento de Verticais - Cidade of September 2017.

- 
341. <sup>cccxli</sup>In May 8, 2017, the city of Salvador inaugurated a system of interconnected smart traffic lights, able to adjust traffic flow in real time through communication between equipment. See: <http://atarde.uol.com.br/transito/noticias/1859571-semaforos-inteligentes-comecam-a-funcionar-em-salvador>. Accessed on 11.14.2017. With the same objective, the City Hall of São Paulo, in partnership with CET, prepares to launch a PPP to modernize the city's traffic light system, implementing a technology that enables them to be operated at a distance. In: Dória vai lançar PPP para modernizar semáforos de SP. O Estado de São Paulo, São Paulo, July 26, 2017. Available at: <http://sao-paulo.estadao.com.br/noticias/geral,doria-deve-lancar-ppp-para-modernizar-semaforos-de-sp,70001906369>. Accessed on 09.12.2017.
342. <sup>cccxlii</sup>Bill no. 1.has been before National Congress since 2011. The Bill has the objective of establishing a provision in the Brazilian Traffic Code (Traffic Code) to obligate the Public Power to install timers in all traffic light, with radars that detect red lights. Proposal available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=507344>. Accessed on 09.21.2017.
343. <sup>cccxliii</sup>These opportunities created by IoT Technologies in relation to traffic are duly described in the partial report Produto 8: Aprofundamento de Verticais - Cidade, of September 2017.
344. <sup>cccxliv</sup>In: Dória anuncia parceria com aplicativos de trânsito para monitorar semáforos. Folha de São Paulo. September 20, 2017. Available at: <http://www1.folha.uol.com.br/cotidiano/2017/09/1920134-doria-anuncia-parceria-com-aplicativo-de-transito-para-monitorar-semaforos.shtml>. Accessed on 09.21.2017.
345. <sup>cccxlv</sup>As seen in the article published by the Rio de Janeiro City Hall in May of 2017: <http://prefeitura.rio/web/guest/exibeconteudo?id=6993721>. Accessed on 09.28.2017.
346. <sup>cccxlvii</sup>The Union is responsible for fostering technological and scientific development to pursue the objectives of this Policy (article 16, VI).
347. <sup>cccxlviii</sup>In situations in which traffic is not limited to the city's territory, article 21 assigns responsibility of road traffic executive bodies and entities of the Union, the States and the Federal District to act within the limits of their power.
348. <sup>cccxlix</sup>Available at: <http://legislacao.prefeitura.sp.gov.br/leis/lei-16050-de-31-de-julho-de-2014/> Accessed on 10.04.2017.
349. <sup>ccc</sup>Available at: <https://diariodotransporte.com.br/2017/06/14/confira-na-integra-o-estatuto-do-pedestre-sancionado-por-doria/>. Accessed on 09.29.2017.
350. <sup>ccc</sup>Available, respectively, at: <http://www.denatran.gov.br/download/Resolucoes/Resolucao4712013.pdf> and <http://www.denatran.gov.br/images/Resolucoes/Resolucao5322015.pdf>. Accessed on 09.29.2017.
351. <sup>ccc</sup>According to article available at: <http://g1.globo.com/rj/regiao-serrana/noticia/2015/08/motoristas-de-nova-friburgo-rj-sao-multados-atraves-de-cameras.html>. Accessed on 09.29.2017.
352. <sup>ccc</sup>Available at: [http://www.denatran.gov.br/download/Resolucoes/RESOLUCAO\\_CONTRAN\\_396\\_11.pdf](http://www.denatran.gov.br/download/Resolucoes/RESOLUCAO_CONTRAN_396_11.pdf). Accessed on 09.29.2017.
353. <sup>ccc</sup>Available at:[http://www.denatran.gov.br/download/Resolucoes/\(Resolu%C3%A7%C3%A3o%20412.2012\).pdf](http://www.denatran.gov.br/download/Resolucoes/(Resolu%C3%A7%C3%A3o%20412.2012).pdf). Accessed on 09.29.2017.
354. <sup>ccc</sup>Available at: <http://www.denatran.gov.br/images/Resolucoes/Resolucao5372015.pdf>. Accessed on 09.29.2017.
355. <sup>ccc</sup>In October 2017, Congressman Eduardo Barbosa (PSDB/MG) proposed Bill no. 8.988/2017, with the main objective of requiring road concession companies to have a security system for installations, integrated with the National Automatic Vehicle Identification System (SINIAV). The Bill also establishes

---

that public security bodies may request data from road concession companies if necessary to conduct police work. Proposal available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2159920>. Accessed on 14.11.2017.

356. <sup>ccclvi</sup> According to article available at: <http://g1.globo.com/carros/noticia/2015/04/exigencia-de-chip-em-veiculos-comeca-valer-daqui-2-meses.html>. Accessed on 09.29.2017.
357. <sup>ccclvii</sup> According to information available at: <http://g1.globo.com/carros/noticia/2015/04/exigencia-de-chip-em-veiculos-comeca-valer-daqui-2-meses.html>. Accessed on 09.29.2017.
358. <sup>ccclviii</sup> A compilation of studies conducted by the World Health Organization shows that an efficient public transportation network helps fight health problems, such as traffic accidents, inactivity, obesity and stress. Available at: <http://www1.folha.uol.com.br/cotidiano/2013/08/1328474-transporte-publico-de-qualidade-reduz-doencas-e-mortes-diz-membro-da-oms.shtml>. Accessed on 09.26.2017.
359. <sup>ccclix</sup> This 2016 research shows three Brazilian cities in the top ten cities with worst traffic in the world: Rio de Janeiro, Salvador and Recife. Available at: <http://brasil.estadao.com.br/noticias/geral,tres-cidades-do-brasil-estao-no-top-10-de-congestionamentos,10000022561>. Accessed on 09.26.2017.
360. <sup>ccclx</sup> According to a research published by the Institute of Transportation and Development Policies and WRI Brazil Sustainable Cities, although the city of São Paulo has the largest public transportation network in Brazil, only 25% of its population lives close to a transportation station. This percentage is considered to be very low when compared to other cities, such as Rio de Janeiro (47%), Mexico City (48%), Beijing (60%), New York (77%) and Paris (100%). Available at: <http://2rps5v3y8o843iokettbxnya.wpengine.netdna-cdn.com/wp-content/uploads/2016/09/2016-09-ITDP-PNT-SP.pdf>. Accessed on 09.26.2017.
361. <sup>ccclxi</sup> According to the description of the IoT solution for mobility of the partial Produto 8: Aprofundamento de Verticais - Cidade, of September 2017.
362. <sup>ccclxii</sup> In this context, an article published by the Indian journal *The Economic Times* states that solutions for vehicle tracking (GPS-based tracking system) enable the improvement of public transportation system operations, generating more trust in the system, since the user is provided with a tool to locate transportation units and plan, in an optimized way, their displacement. Available at: [http://economictimes.indiatimes.com/news/economy/infrastructure/smart-transportation-for-smart-cities/articleshow/48772473.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cpst](http://economictimes.indiatimes.com/news/economy/infrastructure/smart-transportation-for-smart-cities/articleshow/48772473.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cpst). Accessed on 09.25.2017.
363. <sup>ccclxiii</sup> Cidades inteligentes e mobilidade urbana. Caderno FGV Projetos, June/July 2014, year 9, no. 24, p. 59-60. Available at: [http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos\\_fgvprojetos\\_smart\\_cities\\_gwa\\_0.pdf](http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_gwa_0.pdf). Accessed on 09.12.2017.
364. <sup>ccclxiv</sup> A study indicates that an individual who has access to information waits seven minutes less at bus stops – a reduction of about 13% in waiting time. Available at: <http://www.sciencedirect.com/science/article/pii/S0965856411001030>. Accessed on 10.04.2017.
365. <sup>ccclxv</sup> The Israeli app Moovit is an example of data processing within the scope of urban collective public transportation, currently counting on more than 200,000 editors and gaining ground in Brazilian cities. See: <https://smarcitiesworld.net/news/news/public-transport-stops-reaches-mapped-milestone-2259>. Accessed on 11.14.2017.
366. <sup>ccclxvi</sup> In 2016, the São Paulo City Hall determined the expansion of the Integrated Monitoring System, with the introduction of vehicle models with integrated GPS technology to verify the compliance with arrival and departure times. Article published in: <http://sao-paulo.estadao.com.br/noticias/geral,prefeitura-vai-ampliar-fiscalizacao-de-onibus-em-sp,10000024859>. Accessed on 10.04.2017.
367. <sup>ccclxvii</sup> Currently, the crossing of information is carried out by chrono-tachographs present in vehicles that provide the public service. However, the device does not have IoT intelligence and requires the manual

---

reading of collected data. Chrono-tachographs are equipment that indicate and register the speed and distance travelled by the vehicle. According to traffic legislation, they are mandatory devices for passenger vehicles with more than 10 seats (municipal and travel buses); school transportation vehicles; and cargo vehicles with a gross weight of more than 4,536 kilos (CONTRAN Resolutions no. 14/1998, 87/1999 and 92/1999). It is competency of INMETRO to approve existing models and to carry out periodical checks, according to issued guidelines that are available at: <https://cronotacografo.rbmlq.gov.br/legislacao>.

368. <sup>ccclxviii</sup>Scheduled maintenance is shown to avoid traffic jams for more than 800,000 people in London. Big data analysis has been used to quickly respond to cases in the Transport for London system, a service that integrates the management of the city's buses, trains, taxis, roads and ferries. Available at: <http://www.bigdatabusiness.com.br/iot-big-data-e-as-cidades-inteligentes-revolucionando-o-transporte-publico/>. Accessed on 09.26.2017.
369. <sup>ccclxix</sup>Caderno FGV Projetos, June/July 2014, year 9, no. 24. Available at: [http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos\\_fgvprojetos\\_smart\\_cities\\_gwa\\_0.pdf](http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_gwa_0.pdf). Accessed on 09.12.2017.
370. <sup>ccclxx</sup>Mandatory for cities: (i) with more than 20,000 inhabitants; (ii) part of metropolitan regions and urban agglomerations; (iii) that wish to implement instruments of urban policy such as progressive IPTU (property tax); (iv) part of areas of special touristic interest; (v) within areas under influence of enterprises or activities of high regional or national environmental impact; and (vi) part of the national registry of cities with areas subject to landslides of high impact, major flooding or related geological or hydrological activities (article 41, City Statute). For cities with more than 20,000 inhabitants, an Urban Mobility Plan is mandatory, with a focus on non-motorized transportation and an infrastructure that facilitates pedestrian or bicycle travel (article 24, paragraphs 1 and 2 of the National Mobility Policy). Also, in cities with more than 500,000 inhabitants, it is duty of the city to develop an integrated urban transportation plan compatible with the existing master plan (article 41, paragraph 2).
371. <sup>ccclxxi</sup>Master plans available, respectively, at: <http://multimedia.curitiba.pr.gov.br/2015/00175701.pdf>; <http://www.rio.rj.gov.br/dlstatic/10112/139339/DLFE-229591.pdf/LeiComplementar1112011PlanoDiretor.pdf>; <http://www.ibdi-ba.com.br/plano-diretor-de-desenvolvimento-urbano-de-salvadorba/>; and [http://gestaourbana.prefeitura.sp.gov.br/arquivos/PDE\\_lei\\_final\\_aprovada/TEXT0/2014-07-31%20-%20LEI%2016050%20-%20PLANO%20DIRETOR%20ESTRAT%C3%89GICO.pdf](http://gestaourbana.prefeitura.sp.gov.br/arquivos/PDE_lei_final_aprovada/TEXT0/2014-07-31%20-%20LEI%2016050%20-%20PLANO%20DIRETOR%20ESTRAT%C3%89GICO.pdf). Accessed on 10.06.2017.
372. <sup>ccclxxii</sup>Legislative wording available at: [http://www.planalto.gov.br/ccivil\\_03/leis/LEIS\\_2001/L10257.htm](http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10257.htm). Accessed on 09.29.2017.
373. <sup>ccclxxiii</sup>As indicated by the partial report Produto 8: Aprofundamento de Verticais - Cidade, September 2017.
374. <sup>ccclxxiv</sup>Article available at: <https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/>. Accessed on 10.04.2017.
375. <sup>ccclxxv</sup>Article available at: <http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/>. Accessed on 10.04.2017.
376. <sup>ccclxxvi</sup>Available at: [http://www.denatran.gov.br/images/Portarias/2016/Portaria0152016\\_nova.pdf](http://www.denatran.gov.br/images/Portarias/2016/Portaria0152016_nova.pdf). Accessed on 10.06.2017.
377. <sup>ccclxxvii</sup>See: <http://www.serpro.gov.br/menu/nosso-portfolio/por-publico/portfolio-para-empresas>
378. <sup>ccclxxviii</sup>In Uruguay, the exceptions for the requirement of obtaining consent to disclose personal information to third parties are: (i) determination provided by law; (ii) data from public and accessible sources; (iii) when the disclosure is essential for the development of governmental functions; (iv) when only name, last name, identity document, nationality, address and date of birth are shared; (v) when data is provided by contractual, scientific or professional relationship of the data subject and is necessary for the contract's compliance; (vi) for reasons of public health and hygiene, emergency or necessary for epidemic studies, as long as identities are preserved by dissociation mechanisms; (vii) if dissociation processes are

---

applied and impede the identification of data subjects. Source:  
[https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/e23f0f93-1004-4b65-833f-d1f74c347756/guia-4-web.pdf?MOD=AJPERES&CONVERT\\_TO=url&CACHEID=e23f0f93-1004-4b65-833f-d1f74c347756](https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/e23f0f93-1004-4b65-833f-d1f74c347756/guia-4-web.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=e23f0f93-1004-4b65-833f-d1f74c347756) Accessed on 10.04.2017.

379. <sup>ccclxxxix</sup>The advantages of using blockchain in transportation technologies are listed by Yong Yuan and Fei-Yue Wang in Towards Blockchain-based Intelligent Transportation Systems, available at: [https://www.researchgate.net/publication/311919998\\_Towards\\_blockchain-based\\_intelligent\\_transportation\\_systems](https://www.researchgate.net/publication/311919998_Towards_blockchain-based_intelligent_transportation_systems).
380. <sup>ccclxxx</sup>On this topic, see: MIZUKAMI, Pedro Nicoletti; LEMOS, Ronaldo. From Free Software to Free Culture: The Emergence of Open Business. Access to Knowledge in Brazil: New Research on Intellectual Property, Innovation and Development, p. 13-39, 2010. Available at: <http://klangable.com/uploads/books/A2KBrazil.pdf#page=27> Accessed on 10.09.2017.
381. <sup>ccclxxxii</sup>See: Estudo sobre software livre, commissioned by the Brazilian National Institute of Information Technology (ITI): <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2673/FGV-CTS%20-%20Software%20livre.pdf?sequence=1> Accessed on 09.10.2017.
382. <sup>ccclxxxiii</sup>Available at: <https://leismunicipais.com.br/SP/SAO.CARLOS/LEI-12883-2001-SAO-CARLOS-SP.pdf>. Accessed on 10.09.2017.
383. <sup>ccclxxxiv</sup>Available at: <http://mobilab.prefeitura.sp.gov.br/projetos/>. Accessed on 10.09.2017.
384. <sup>ccclxxxv</sup>For more information, see: <https://www.nexojournal.com.br/expresso/2016/11/03/Por-que-o-software-livre-vai-perder-espaco-no-governo-federal>. Accessed on 10.06.2017.
385. <sup>ccclxxxvi</sup>For more information, see: <https://www.pcmag.com/encyclopedia/term/37856/api>. Accessed on 10.04.2017.
386. <sup>ccclxxxvii</sup>See: <http://thecityfixbrasil.com/2016/02/12/dados-de-transito-em-tempo-real-sao-bons-para-as-pessoas-e-para-as-cidades-o-que-esta-atrasando-esse-tecnologia/>
387. <sup>ccclxxxviii</sup>See: <http://kit.dados.gov.br/>
388. <sup>ccclxxxix</sup>For more, see: [http://dados.prefeitura.sp.gov.br/pt\\_PT/](http://dados.prefeitura.sp.gov.br/pt_PT/)
389. <sup>ccclxxxix</sup>Wording available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2150508>. Accessed on 11.14.2017.
390. <sup>cccxci</sup>Law no. 8.248/1991 (Computer Law) must also be observed, as it addresses training and competitiveness in the computer and automation sector. Among its provisions are guidelines for the Administration to give preference to the acquisition of products and services developed by national technology (article 3). It is interesting to note that the Law presents a list of goods and services considered as Information Technology and Communication, such as electronic components; machines; equipment and devices based on digital techniques; computer programs; equipment and devices; and technical services related to these goods (article 16-A). This regulation was changed by Provisional Measure no. 810/2017, which included companies that develop or manufacture ITC goods and services that invest in research, development and innovation activities related to this sector, through tax incentives provided for by Law no. 8.191/1991, which establishes the exemption of the Tax on Manufactured Products – IPI.
391. <sup>cccxci</sup>Ordinance no. 141/2014 also stipulates that the Administration must require private entities that provide ITC services to adopt the Interoperability Standards of the Electronic Government (e-PING), and the use of encrypting techniques for confidential information and access controlling tools. Available at: [https://www.governoeletronico.gov.br/documentos-e-arquivos/e-PING\\_v2017\\_20161221.pdf/at\\_download/file](https://www.governoeletronico.gov.br/documentos-e-arquivos/e-PING_v2017_20161221.pdf/at_download/file).
392. <sup>cccxci</sup>Difficulties in identifying the exact understanding of these two entities must be considered, given that neither refers to Decree no. 8.135 nor Ordinance no. 141 in their publications nor press conferences.



---

Among the recent activities in relation to technology solutions is contracting cloud computing services, to be further described in the pages that follow.

393. <sup>cccxciii</sup>The Administration must also require that participants in IT solutions bidding processes demonstrate, during qualification phase, that they are certified as a public or private entity credited by INMETRO in three different aspects: (i) security of users and facilities; (ii) electromagnetic compatibility; and (iii) energy consumption (article 3).
394. <sup>cccxciv</sup>The SISP central body has the fundamental role of developing an Information Technology and Communication General Strategy, published annually, and which must assist in development of information technology master plans (known as PDTI) by the bodies and entities that are part of SISP (article 3). As in Decree no. 1.048/1994 and Decree no. 7.579/2011.
395. <sup>cccxcv</sup>It is worth noting that, beyond signing terms of reference for the basic project, the planning process must include a planning team, a preliminary technical study and an analysis of hire-related risks (article 9) from the start.
396. <sup>cccxcvi</sup>Specific instruction that establishes that the selection of IT solutions characterized as common goods or services must adopt the “reverse auction” model, preferably in electronic form (article 26, only paragraph).
397. <sup>cccxcvii</sup>The first movement to regulate information security aspects goes back to the year 2000, with the enactment of Decree no 3.505, which established the Information Security Policy for Federal Public Administration institutions.
398. <sup>cccxcviii</sup>According to data from the Ministry of Communications, published in 2014, the Information Security Cabinet had, until that moment, issued 4 Decrees, 3 Normative instructions, 21 Complementary standards to IN 01 – SIC, and 1 complementary standard to IN 02 – Security Credentials.
399. <sup>cccxcix</sup>In the Product 8 report on information security, we address the role of Information Security Cabinet in information security within the exclusive sphere of the Federal Public Administration and, specifically, in the security management of critical infrastructures of which it is part. Decree no. 7.009/2009 attributed this issue to the Chamber of Foreign Relations and National Defense (“CREDEN”), presided by the Chief Minister of the Information Security Cabinet. In 2010, the Communications and Information Security Department (“DSIC”), also linked to the Cabinet, published the *Guia de Referência Para a Segurança das Infraestruturas Críticas da Informação* (Reference Guide for the Security of Critical Information Infrastructures), a current reference on related institutional models. Available at: [http://dsic.planalto.gov.br/documentos/publicacoes/2\\_Guia\\_SICI.pdf](http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf).
400. <sup>cd</sup>Available at: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15CC7BCB8015CEA6BFBA152F8>. Although the contracting of this event is suspended by Security Mandate no. 1011543-07.2017.4.01.3400, the controversy does not address the object the contract, but a possible violation of the proper process in one of its phases (the use of robots in the auction competition phase, violating the minimum seconds interval between bids provided in Normative Instruction no. 03 of 10.04.2013).
401. <sup>cdi</sup>According to the NIST SP 500-292 definition, *cloud broker* is an entity that manages the use, execution and provision of cloud computing services and also negotiates the relationships between service providers and cloud consumers. Available at: [http://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=909505](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505). Accessed on 01.15.2018.
402. <sup>cdii</sup>The terms of the Ministry of Planning, however, require both cloud computing service operators and integrators to have servers physically located in Brazil.
403. <sup>cdiii</sup>Available at: <https://www.governoeletronico.gov.br/documentos-e-arquivos/Portaria%20MP-STI%20no%2020%20de%2014%20de%20junho%20de%202016.pdf>.
404. <sup>cdiv</sup>Available at: <https://www.governoeletronico.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf>.

- 
405. <sup>cdv</sup> Available at: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15005860201501E7CDF5B41AC>.
406. <sup>cdvi</sup> According to the definition adopted by the Ministry of Planning in the annex of Ordinance no. 20/2016, which provides general guidelines and good practices for contracting cloud computing services, the hybrid cloud is a composition of two cloud infrastructures (private and public) interconnected by appropriate technologies that allow the migration of applications and data between the clouds.
407. <sup>cdvii</sup> In this context, the Court of Audit Decision no. 1.739/2015 highlights the need for adequate data migration processes for the eventual need to change service providers. In addition, the Court recommends the use of modular bundles, open standards in data services and use and transparency in migration processes and costs.
408. <sup>cdviii</sup> Decision no. 1.739/2015 prevails, considering that the Court of Audit recommended the establishment of clear limits related to the rights of cloud computing service providers to access and use governmental data.
409. <sup>cdix</sup> NC GSI/PR no. 14, item 5.2.2. The Brazilian legislation prevails over any other, in order to ensure legal guarantees to a service contractor and owner of information stored in the cloud.
410. <sup>cdx</sup> The TCU understands that not all cloud computing services with servers located outside of Brazil are capable of guaranteeing that any eventual foreign legislation would not prevail over national legislation during the provision of their services. The Court suggests that contracts regarding this type of service provision must clearly establish in which countries data is stored. Union Court of Audit (TCU), Decision no. 1739 of 2015, Annex I.
411. <sup>cdxi</sup> Therefore, it is not our purpose to present guidelines for public managers or potential contracted service providers, neither do we intend to indicate normative guidelines to the bodies endowed with the referred normative competency.
412. <sup>cdxii</sup> Models and types are not synonyms. Models are types of bidding processes and types are the decision criteria used to hire them.
413. <sup>cdxiii</sup> Federal Supreme Court, Full Court, ADI 3059/RS. Rel. Min. Luiz Fux, d.j., 04.09.2015.
414. <sup>cdxiv</sup> Federal Supreme Court, Full Court, ADI 3670/DF, Rel. Min. Sepúlveda Pertence, d.j. 04.02.2007.
415. <sup>cdxv</sup> Another relevant case is the trial of the bidding law of the city of São Paulo (Federal Supreme Court, Monocratic Decision, ADI 4116/SP, Rel. Min. Gilmar Mendes, d.j. 07.20.2012), that inverts phases of qualification and proposal analysis provided in the federal law (Law no. 8.666/1993). This state law, as well as the law in Bahia, Paraná and a municipal law of São Paulo, follow a trend established by the auction type of bidding, initially developed by the National Telecommunications Agency – ANATEL. The inversion of procedures was questioned on its possibility of becoming a new bidding modality and, therefore, not subject to local deliberation. Its merits were not trialed, and the doubt remains until today.
416. <sup>cdxvi</sup> VOJVODIC, Adriana et al. *Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação: Análise de Entraves e Propostas para Aquisição*. São Paulo: Iniciativa para Inovação na Educação Brasileira e InternetLab, 2015. Available at: [http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB\\_CompraseInovacaoEduc\\_v6-1.pdf](http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf). Accessed on 01.17.2018.
417. <sup>cdxvii</sup> One existing alternative to the efficiency and capacity issues of the public manager would be the institution of a central procurement body, with the necessary expertise and institutional structure to contract ICT. This body would have better conditions to identify the products available in the market and to coordinate acquisitions to enhance its capacity to negotiate with suppliers. FIUZA, Eduardo P. S.; MEDEIROS, Bernardo de A. *A Agenda Perdida das Compras Públicas: Rumo a uma Reforma Abrangente da Lei de Licitações e do Arcabouço Institucional*. Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada - IPEA, August, 2014, p. 91-92. Available at: [http://repositorio.ipea.gov.br/bitstream/11058/3362/1/td\\_1990.pdf](http://repositorio.ipea.gov.br/bitstream/11058/3362/1/td_1990.pdf). Accessed on 01.17.2018.



- 
418. <sup>cdxviii</sup>In its manifestation during the Public Hearing realized by the study, Telefônica Brasil suggested a possible solution to the challenge related to developing an auction notice: “It would be interesting to have bidding “reference guides” developed by the IoT Chamber, which may be used by the public power, ensuring the quality of the hired services. This would reduce the risk of the government hiring a solution that is not the best (technically and economically) for society.”
419. <sup>cdxix</sup>A similar concern was raised during the IoT Public Consultation, in which players such as Unitec indicated insufficient knowledge among Administration staff on technical concepts and benefits offered by the employment of IoT devices as one of the obstacles to be faced by public entities in the adoption of solutions based on M2M and IoT technology and communication. Available at: <http://www.participa.br/portal/blog/consulta-publica-iot>. Accessed on 01.19.2018.
420. <sup>cdxx</sup>VOJVODIC, Adriana et al. *Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação: Análise de Entraves e Propostas para Aquisição*. São Paulo: Iniciativa para Inovação na Educação Brasileira e InternetLab, 2015. Available at: [http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB\\_CompraseInovacaoEduc\\_v6-1.pdf](http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf) Accessed on 01.17.2018.
421. <sup>cdxxi</sup>According to a study on ICT contracted for education: “The interviews showed an estimate of 18 to 24 months to sell a product to the government. Even procedures enabled by the FNDE acts on price registration, which are more efficient, were not enough to ensure the purchase of products with non-obsolete technology”. VOJVODIC, Adriana et al. *Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação: Análise de Entraves e Propostas para Aquisição*. São Paulo: Iniciativa para Inovação na Educação Brasileira e InternetLab, 2015, p. 35. Available at: [http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB\\_CompraseInovacaoEduc\\_v6-1.pdf](http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf) Accessed on 01.17.2018.
422. <sup>cdxxii</sup>In this context, a report on ICT contracts for education says: “Other than that, the need to prove that the price was within market parameters was mentioned in some interviews. This suggests that there is no adequate routine to contract single products, imposing the same formality criteria used for hiring in the competitive markets.” VOJVODIC, Adriana et al. *Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação: Análise de Entraves e Propostas para Aquisição*. São Paulo: Iniciativa para Inovação na Educação Brasileira e InternetLab, 2015, p. 35. Available at: [http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB\\_CompraseInovacaoEduc\\_v6-1.pdf](http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf) Accessed on 01.17.2018.
423. <sup>cdxxiii</sup>Aquisição de Tecnologia Educacional pelo Setor Público: Entraves e Caminhos para Estimular o Ecosistema de Inovação no Brasil. Iniciativa da Inovação na Educação Brasileira - IIEB, 2015, p. 39. Available at: [http://www.cieb.net.br/wp-content/uploads/2016/06/082015\\_IIEB-Relatorio-Compras-Executivo\\_WEB\\_AFF.pdf](http://www.cieb.net.br/wp-content/uploads/2016/06/082015_IIEB-Relatorio-Compras-Executivo_WEB_AFF.pdf). Accessed on 01.18.2018.
424. <sup>cdxxiv</sup>A study conducted by InternetLab shows the auction being used by the Ministry of Education to hire hardware. Therefore, ICT with more market availability and less innovation potential are more easily bid on using the auction model than other kinds of ICT, such as software. “Since 2008, MEC has conducted 41 bids related to computer science, technology and innovation. Most of them were for internal consumption and the few cases of observed technology acquisitions were usually of hardware and usually made through electronic auction.” VOJVODIC, Adriana et al. *Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação: Análise de Entraves e Propostas para Aquisição*. São Paulo: Iniciativa para Inovação na Educação Brasileira e InternetLab, 2015, p. 14. Available at: [http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB\\_CompraseInovacaoEduc\\_v6-1.pdf](http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf). Accessed on 01.17.2018.
425. <sup>cdxxv</sup>COSTA, Gustavo Vidigal. Pregão para contratação de bens e serviços em Tecnologia da Informação – Sistema (Software) em Gestão Pública. Revista do TCU, n. 119, p. 13-22, 2010.
426. <sup>cdxxvi</sup>This position is adopted by the Union Court of Audit. In Decision no. 2.471/2008-TCU-Plenário, item 9.2.2.
427. <sup>cdxxvii</sup>According to the Court of Audit, ICT goods and services with performance and quality standards specifically defined in notices must be bid on using the auction model. As many of these products have been increasingly presenting a more standardized nature, unlike intellectual and artistic products, it is expected that the auction model will be expanded to ICT contracts. According to the Court, not even the

- 
- complexity of these products or their relevance to the Administration may be used as a reason to dismiss their standardization. In SEFTI/TCU Technical Note no. 02/2008, available at:<http://revista.tcu.gov.br/ojs/index.php/RTCU/article/download/284/297>. Accessed on 01.19.2018.
428. <sup>cdxxxviii</sup>Union Court of Audit (TCU), TC 010.123/2003-9, tried on 06/29/2004. Available at: [https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKewjQ7sOzgeLYAhVBDpAKHR3CCOQOFggoMAA&url=http%3A%2F%2Fwww.tcu.gov.br%2FConsultas%2FJuris%2FDocs%2Fjudoc%2FAcord%2F20041215%2FTC-020-353-2003-2.doc&usq=AOvVaw2b8i3\\_di7MaBWjG8XyxDoN](https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKewjQ7sOzgeLYAhVBDpAKHR3CCOQOFggoMAA&url=http%3A%2F%2Fwww.tcu.gov.br%2FConsultas%2FJuris%2FDocs%2Fjudoc%2FAcord%2F20041215%2FTC-020-353-2003-2.doc&usq=AOvVaw2b8i3_di7MaBWjG8XyxDoN). Accessed on 01.18.2018.
429. <sup>cdxxxix</sup>Bill no. 4432/2008, sponsored by Congressman Carlos Zarattini, aims to include within bid exemption possibilities, goods and services of low technological complexity that are essential to strategic activities of national security. The Bill was attached to Bill no. 1.292/1995, which suggests changing the bidding law. The Bill may be accessed at:<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=418926>. Accessed on 01.18.2018.
430. <sup>cdxxx</sup>For more information, see: MIZUKAMI, Pedro Nicoletti; LEMOS, Ronaldo. From free software to free culture: The emergence of open business. Access to Knowledge in Brazil: New Research on Intellectual Property, Innovation and Development, p. 13-39, 2010. Available at: <http://klangable.com/uploads/books/A2KBrazil.pdf#page=27>. Accessed on 09.10.2017.
431. <sup>cdxxxix</sup>See the National Information Technology Institute (ITT) study on free software, available at: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2673/FGV-CTS%20-%20Software%20livre.pdf?sequence=1>. Accessed on 09.10.2017.
432. <sup>cdxxxii</sup>In 2000, the Government had already started to rationalize the costs of contracted software, issuing Presidential Decree no. 18/00, which instituted the Electronic Government Executive Committee.
433. <sup>cdxxxiii</sup>For more information, see: TEIXEIRA, Raphael L. C. J. A Contratação de Licenciamento de Software na Administração Pública. *Questio Juris*, v. 4, n. 01, 2011, p. 619. Available at: <http://www.e-publicacoes.uerj.br/index.php/quaestiojuris/article/view/10201>. Accessed on 01.18.2018.
434. <sup>cdxxxiv</sup>An example is Law no. 12.883, of 2001, issued by the city of São Carlos in the state of São Paulo to determine that the Mayor's Office must prioritize programs with open, free and unrestricted source codes. Available at:<https://leismunicipais.com.br/SP/SAO.CARLOS/LEI-12883-2001-SAO-CARLOS-SP.pdf>. Accessed on 01.17.2018.
435. <sup>cdxxxv</sup>As in the article. 37, XXI, of the Federal Constitution and article 3 of Law no. 8.666/1993.
436. <sup>cdxxxvi</sup>STF, Precautionary Measure in Direct Action of Unconstitutionality 3.0591-RS, Judge Carlos Ayres Britto, d.j. 04.15.2004.
437. <sup>cdxxxvii</sup>The argument used by the Court was used in the analysis of the constitutionality of the Rio Grande do Sul law that established the preference for free software contracting by its public state bodies. Rio Grande do Sul Law no. 11.871/2002, article 1, *caput*. “(...) Will preferably use in their systems and equipment, open and free programs with no restrictions of ownership, authorization, alteration and distribution”. Cf. FERRAZ JÚNIOR, Tércio Sampaio. *Software Livre: a Administração Pública e a Comunhão do Conhecimento Informático*. Revista de Direito Público da Economia - RDPE, Belo Horizonte, year 3, n. 11, July/September. 2005, p. 190.
438. <sup>cdxxxviii</sup>Bills have already been presented aiming to ensure the isonomy of opportunities between suppliers in situations of parallel purchases of technologic solutions, among them Bill no. 167/2007 and Bill no. 1739/2003, both filed.
439. <sup>cdxxxix</sup>Cf. FERRAZ JÚNIOR, Tércio Sampaio. *Software Livre: a Administração Pública e a Comunhão do Conhecimento Informático*. Revista de Direito Público da Economia - RDPE, Belo Horizonte, ano 3, n. 11, July/September. 2005, p. 186.

- 
440. <sup>cdxli</sup>For better understanding, an analogy is made to the duties of purchasing or renting a house: the choice for purchase or rent is based on the expectations of the contractor and on the design of the contract, not on the characteristics of the house. The same happens in the choice for open or private software: the hire is not related to the technical capacities of the software, but to the definition of the bidding process and to the purpose of the Administration.
441. <sup>cdxlii</sup>This concern alludes to the existing legal provision of the national IT policy of “forbidding monopolistic situations, of right or fact” (article 2, IV, of Law no. 7.232/1984). The software market, based on technology and information, has a monopolistic tendency in the capacity to create a “networked” virtuous cycle: the more people use a determined product or service, the more others start to use it. As a result, leading innovative products end up owning a large market share (winner-takes-most).
442. <sup>cdxliii</sup>Supreme Federal Court, Full Court, ADI 3059/RS. Judge Luiz Fux, d.j., 04/09/2015.
443. <sup>cdxliv</sup>As part of continued development of the public surveillance system possibilities, the following are being integrated into existing CCTV high-resolution video systems equipment; high sensitivity microphones; cameras with OCR technology and facial recognition; and sensors of all kinds. For a technical description of the solutions, see the descriptive section of the Appendix
444. <sup>cdxlv</sup>In a report for the newspaper *The Guardian*, the UK Commissioner for Security has similar concerns about the development of monitoring technologies in the cities of the country: “The increasing use of surveillance technology – including body-worn video, drones and vehicle plate recognition systems – risks changing the ‘psyche of the community’ by reducing individuals to trackable numbers in a database, the government’s CCTV watchdog has warned.” Available at: <https://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent>. Accessed on: September 15, 2017. In the state of California, residents are concerned with the existence of the *Domain Awareness Center* (DAC), a surveillance center for monitoring the port and airport of the city of Oakland. The City Council proposed an expansion of the system, so that it would stream images transmitted by closed circuits from traffic cameras; vehicle plate reading techniques; gunshot detectors; and also other technologies capable of including the entire city. Available at: <http://edition.cnn.com/2014/05/26/tech/city-of-tomorrow-video-data-surveillance/index.html>. Accessed on: 15.09.2017.
445. <sup>cdxlvi</sup>According to the book published by the *Berkman Center for Internet & Society* at Harvard University, IoT technology devices are designed to grow progressively, and they have the potential to dramatically change the surveillance landscape. The images, videos, and audios collected by these objects can provide real-time intercepts and fact checks after their occurrence (page 3). Available at [https://cyber.harvard.edu/pubrelease/dont-panic/Dont\\_Panic\\_Making\\_Progress\\_on\\_Going\\_Dark\\_Debate.pdf](https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf). Accessed on: September 6, 2017.
446. <sup>cdxlvii</sup>José Afonso da Silva classifies “public security” as an “activity to vigilance, prevention and repression of deleterious conduct”. In: SILVA, José Afonso da. *Curso de direito constitucional positivo*. 34 ed. São Paulo: Malheiros, 2011, p. 779.
447. <sup>cdxlviii</sup>Federal Supreme Court, RE 559.646 AgR, by Judge Ellen Gracie, j. 7-6-2011, 2ª T, DJE of 24-6-2011.
448. <sup>cdxlix</sup>“The integration of a variety of sensors (audio sensors and chemical, biological and radiological sensors) with CCTV technology has been categorized in Europe as “Massively Integrated Multiple Sensor Installations” (MIMSI). In the US, the term for MIMSI is “Domain Awareness System” (DAS).” In: KLITOU, Demetrius. *Privacy-invading technologies and privacy by design: Safeguarding privacy, liberty and security in the 21st century*. The Hague: Asser Press, 2014, p. 116.
449. <sup>cdxli</sup>According to Hely Lopes Meirelles, “traditionally, the police in a material sense is conceptualized from the position of supremacy of the Public Power in imposing limits on the actions of individuals in order to preserve public order”. MEIRELLES, Hely Lopes. *Estudos e pareceres de direito público*, v. II, São Paulo: RT, 1979/1995, p. 6. In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. *Constituição Federal comentada e legislação constitucional*. 6 ed. São Paulo: Editora Tribunal dos Tribunais, 2017, p. 1022.

- 
450. <sup>cdl</sup> “Public security consists of a situation of preservation or re-establishment of this social coexistence that allows all to enjoy their rights and to exercise them without hindrance from others”. In SILVA, Jose Afonso da. Curso de direito constitucional positivo. 34 ed. Sao Paulo: Malheiros, 2011 p. 779.
451. <sup>cdli</sup> According to Pedro Machete, “All police activity must be governed by the principle of prohibition of excess, whose existence is fundamental to control the performance of public powers in the Constitutional State, assuming, especially with regard to fundamental rights, the role of the main instrument of control of restrictive action of individual freedom”. In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. Constituição Federal comentada e legislação constitucional. 6 ed. São Paulo: Editora Tribunal dos Tribunais, 2017, p. 1023.
452. <sup>cdlii</sup> Detecta is a system for identifying vehicles and suspicious activities (such as theft and robberies) through monitoring cameras and OCR cameras, implemented in 2014 by the Secretary of Public Security of the State of São Paulo.
453. <sup>cdliii</sup> The Court of Audit (TCA) of the State of São Paulo. Book of Surveillance of Operational Nature, Solution of Situational Consciousness - TCA no. 17.941/026/2015, Counselor Sidney Estanislau Beraldo. Available at: <https://www4.tce.sp.gov.br/sites/tcesp/files/downloads/detecta.pdf>. Accessed on September 15, 2017. The purpose of the book is to "verify if acquisition of Detecta met the demand for smart software that automates the process of video monitoring of public spaces and reduces the number of people dedicated to monitoring the cameras; if it is operating with the functionality provided in the contract; as well as ensuring the reliability and security of information, and evaluating results in planning, prevention and police investigation activities "(pages 7-8).
454. <sup>cdliv</sup> Source: <http://edition.cnn.com/2014/05/26/tech/city-of-tomorrow-video-data-surveillance/index.html>. Accessed on: September 15, 2017.
455. <sup>cdlv</sup> KLITOU, Demetrius. Privacy-invading technologies and privacy by design: Safeguarding privacy, liberty and security in the 21st century. The Hague: Asser Press, 2014, p. 119.
456. <sup>cdlvii</sup> The *European Forum for Urban Security* was founded in 1987 under the auspices of the European Council, as the only European network of local and regional authorities dedicated to urban safety, including some 250 local and regional authorities from 16 countries. Available at: <https://efus.eu/en/about-us/about-efus/public/1450/>. Accessed on: September 15, 2017.
457. <sup>cdlviii</sup> Available at: [https://issuu.com/efus/docs/cctv\\_charter\\_pt](https://issuu.com/efus/docs/cctv_charter_pt). Accessed on: September 15, 2017.
458. <sup>cdlix</sup> Available in Portuguese at: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=EN>. Accessed on: 09.10.2017.
459. <sup>cdlix</sup> (26) The processing of personal data must be done in a lawful, fair and transparent manner with the natural persons concerned, and exclusively for the specific purposes as provided for by law. This does not in itself prevent law enforcement authorities from engaging in activities such as undercover investigations or video surveillance. Such activities may be conducted for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or enforcing criminal sanction, including the safeguarding and prevention of threats to public security, provided they are provided for by law and are a necessary and proportionate measure in a taking due account of the legitimate interests of the natural person concerned. Fair treatment, which is one of the principles of data protection, is a distinct notion of the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Individuals should be made aware of the risks, rules, guarantees and rights associated with the processing of their personal data and the means available to them to exercise their rights regarding the processing of such data. In particular, the specific effects of the treatment should be explicit and legitimate and should be determined at the time of collection of personal data. Personal data should be appropriate and relevant for the purposes for which data is being processed. It is particularly important that personal data collected are not excessive in scope or kept for longer than is necessary for the purposes for which they are being processed. Personal data should only be processed if the purpose for accessing them cannot otherwise be reasonably achieved by other means. To ensure that data is kept only for the period considered necessary, the data controller shall set time limits for deleting or for periodic review. Member States shall provide for appropriate safeguards applicable to personal data



---

was a simplified analysis process for the products considered low risk, considering that by simplifying the pre-market process, greater emphasis would be placed on controlling the post-market stages of products.

475. <sup>cdlxxv</sup>Annex II - Technical Dossier of Medical Products: "1. The Technical Dossier need not correspond to a physical or electronic file containing all the information described below, and may be composed of references to documents and information that comprise other files or records of the Company's Quality System, which should be available for oversight by the National Health Surveillance System. "
476. <sup>cdlxxvi</sup>Resolution RDC no. 185, of 2001:
477. "13. The registry of health products will be valid for 10 (ten) years, starting from the day of its publication in the Official Diary of the Union, and may be invalidated successively for the same period. (Text given by Resolution - RDC No. 211, of January 22, 2018). "
478. <sup>cdlxxvii</sup>In the US, there already exist regulations for combined products, through the U.S Food & Drug Administration – FDA. "Combination products are therapeutic and diagnostic products that combine drugs, devices, and/or biological products. FDA expects to receive large numbers of combination products for review as technological advances continue to merge product types and blur the historical lines of separation between FDA's medical product centers, which are made up of the Center for Biologics Evaluation and Research (CBER), the Center for Drug Evaluation and Research (CDER), and the Center for Devices and Radiological Health (CDRH). Because combination products involve components that would normally be regulated under different types of regulatory authorities, and frequently by different FDA Centers, they raise challenging regulatory, policy, and review management issues. Differences in regulatory pathways for each component can impact the regulatory processes for all aspects of product development and management, including preclinical testing, clinical investigation, marketing applications, manufacturing and quality control, adverse event reporting, promotion and advertising, and post-approval modifications." Available at <https://www.fda.gov/CombinationProducts/AboutCombinationProducts/default.htm>
479. <sup>cdlxxviii</sup>Available at: <http://portal.anvisa.gov.br/documents/33912/264673/Software+as+a+Medical+Device.pdf/df5e4fa8-4d45-4f7d-ba67-bfd49c1f3bcd>. Accessed on November 16, 2017.
480. <sup>cdlxxix</sup>Available at "IMDRF/SaMD WG/N10FINAL:2013, *Title: Software as a medical device: key definitions*". Accessed on November 16, 2017.
481. <sup>cdlxxx</sup>Available at "IMDRF/SaMD WG/N12FINAL: 2014, *Title: Software as a medical device: possible framework for risk categorization and corresponding considerations*". Accessed on 16.11.2017.
482. <sup>cdlxxxi</sup>Available at "IMDRF/SaMD WG/N23 FINAL:2015. *Title: Software as a Medical Device: application of quality management system*." Accessed on 16.11.2017.
483. <sup>cdlxxxii</sup>Available at IMDRF/SaMD WG/N41FINAL:2017. *Title: Software as a Medical Device: clinical evaluation*. Accessed on November 16, 2017.
484. <sup>cdlxxxiii</sup>Available at: <https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>. November 16, 2017.
485. <sup>cdlxxxiv</sup>Law no. 3.268, of September 30, 1957: "Art. 2 The Federal Council and the Regional Councils of Medicine are the supervisory organs of professional ethics throughout the Republic and also serve as judges and disciplinarians of the medical profession, responsible for ensuring, and with all means at their disposal, perfect ethical performance of medicine and to esteem the profession and those who exercise it legally. "
486. <sup>cdlxxxv</sup>Exposition of Motives of CFM Resolution No. 1.821/2007: "The patient's medical record in any storage medium is the physical property of the institution where the patient is assisted, whether it is a health unit or a doctor's office. The data contained therein belongs to the patient, and data can only be disclosed with his authorization or that of the party responsible for him, or for due legal or just cause. This data must be permanently available so that, when requested by the patient or his legal representative, authentic copies of the information relevant to him is supplied (...) With this, the Federal Council of



---

Medicine recognizes the importance of using computerized systems for the safekeeping and handling of patient records and for the exchange of health information, as well as the digitization of medical records, as a tool for modernization, with consequent improvement in patient care. It is the duty of the CFM to assure to the doctor ample legal support in the utilization of these systems, which is the reason for which it publishes this Resolution. "

487. <sup>cdlxxxvii</sup>The resolution, in Article 1, defines telemedicine as "*the exercise of medicine through the use of interactive methodologies of audiovisual communication and data, with the purpose of health care, education and research*". Given its interpretation as a medical act, telemedicine services must offer appropriate technological infrastructure and comply with the CFM's technical standards regarding storing, handling and transmission of data, and confidentiality, privacy and professional confidentiality. Available at: [http://portal.cfm.org.br/index.php?option=com\\_content&view=article&id=1087:&catid=3](http://portal.cfm.org.br/index.php?option=com_content&view=article&id=1087:&catid=3). Accessed on: September 25, 2017.
488. <sup>cdlxxxviii</sup>Available at: <http://www.bndes.gov.br/wps/wcm/connect/site/e614e9a3-053b-42d4-853a-6b4aa406e31f/produto-3-analise-de-oferta-e-demanda-relatorio-horizontal-ambienteregulatorio.pdf?MOD=AJPERES&CVID=IWrmVIj&CVID=IWrmVIj&CVID=IWrmVIj>, pages 33 to 52. Accessed on November 16, 2017.
489. <sup>cdlxxxix</sup>Bill presented on June 13, 2012 by Congressman Milton Monti of PR/SP.
490. <sup>cdlxxxix</sup>Senate Bill no. 330 presented on August 13, 2013 by Senator Antonio Carlos Valadares of PSB/SE.
491. <sup>cdxc</sup>Senate Bill no. 5.276 presented on May 13, 2016 by the Executive Power and attached to Bill no. 4060/2012.
492. <sup>cdxci</sup> On the 2017 International Seminar:  
<http://portal.anvisa.gov.br/documents/33912/264673/Software+as+a+Medical+Device.pdf/df5e4fa8-4d45-4f7d-ba67-bfd49c1f3bcd>. Accessed on November 16, 2017.
493. <sup>cdxcii</sup>On the FDA's cybersecurity policy:  
<https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>. Accessed on November 16, 2017.
494. <sup>cdxciii</sup> "FDA recommendations for mitigating and managing cybersecurity threats include: - Medical device manufacturers and healthcare facilities should take steps to ensure appropriate safeguards. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
495. - Hospitals and healthcare facilities should evaluate their network security and protect their hospital systems.
496. <sup>cdxciv</sup> "Article 7\_\_Internet access is essential to the exercise of citizenship and the following rights are assured to the user: (...) IX – express consent on personal data collection, use, storage and processing, which must occur separately from other contractual clauses",
497. <sup>cdxcv</sup>*Privacy by design* is a concept that provides for an approach for development of projects, products and services that promotes care in the privacy and personal data protection of users from inception. For more information: <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/>
498. <sup>cdxcvi</sup> "Article 4. Every person has the right to humanized and supportive care, provided by qualified professionals in a clean, comfortable environment that is accessible to all. Single paragraph. It is the right of the individual, in the health services network, to have humanized, supportive care, free from any discrimination, restriction or negotiation in virtue of age, color, ethnicity, religion, sexual orientation, gender identity, economic or social condition, state of health, anomaly, pathology or disability, assuring: (...) III – during appointments, diagnostic, preventive, surgical, therapeutic or hospitalization procedures, the following: (...) (e) confidentiality of every and any personal information
499. <sup>cdxcvii</sup>"Article 8. It is the duty of every citizen to communicate the local sanitary authority of the occurrence of fact, proven or presumed, of transmissible disease, it being obligatory to doctors and other health

---

professionals in the exercise of the profession, as well as to others responsible for public or private health organizations and establishments, the notification of suspicious or confirmed cases of related diseases as in Article 7. (...) Article 10. The compulsory notification of diseases is of confidential character, obligating sanitary authorities. Single paragraph. The identity of the patient with diseases referred to in this article, beyond medical and sanitary scope, may only become effective under exceptional character, in case of high risk to the community, at the discretion of the sanitary authority and with previous knowledge of the patient or person responsible”.

500. <sup>cdxcviii</sup>The Ordinance establishes the legal references and standards on information security of the Ministry of Health: “Article 6. The actions of Information and Communication Security of the Ministry of Health must observe the following legal and normative requirements: I - Decree no. 1.171, of June 22 of 1994, which approves the Professional Ethics Code of the Public Civil Servant of the Federal Executive Branch; II - Decree no. 3.505, of June 13 of 2000, which institutes the Information Security Policy in the organs and entities of the Federal Public Administration; III - Law no. 9.983 of July 14 of 2000, which alters Decree-Law no. 2.848 of September 7 of 1940 (Criminal Code), that provides for classification of computerized crimes against Social Security and Public Administration, IV - Article 1.016 of Law no. 10.406 of January 10 of 2002 (Civil Code), which provides that administrators jointly respond to society and third parties who have suffered harm due to fault in the development of their functions; V - Ordinance no. 589 of May 20 of 2015, that institutes the National Information and Health Computing Policy (PNIS); VI – Normative Instruction no. 01 of June 13 of 2008, of the National Defense Council and its respective Complementary Standards published in the Official Diary of the Union (DOU) by the Department of Information and Communication Security of the Institutional Security Chamber of the Presidency of the Republic (DSIC/GSIPR), which regulates the management of information and communication security in the scope of the Federal Public Administration; VII – Ordinance no. 2.072 of August 31 of 2011, which redefines the Information and Health Computing Committee (CIINFO) in the scope of the Ministry of Health; VIII – Law no. 12.527 of November 18 of 2011, that provides on the procedures to be observed by the Union, States, Federal District and Municipalities, for assuring access to information; IX – Decree no. 7.724, of May 16 of 2012, which regulates Law no. 12,527 of November 18 of 2011; X - Decree no. 7.845 of November 14 of 2012, that regulates procedures for the accreditation of security and treatment of information classified under any degree of confidentiality, and disposes on the Accreditation and Security Nucleus; XI - Norm NBR ISO/IEC 27002:2013 – Code of Conduct for Management of Security of Information; and XII - ISO 31.000:2009 – Guidelines to implement risk management.”

501. <sup>cdxcix</sup>The publication of the Ordinance considered Judgement no. 1.233 – (Court of Audit of the Union)/TCU/2012, which provides for the adoption of standards for Information and Communications Security and Judgement no. 3.015-TCU/2014, which provides for the general strategy of Information Security.

<sup>d</sup> Article 10. Every public agent of the Ministry of Health is responsible for the safety of information and communication assets that are under its responsibility and for all acts executed with their identities such as: user identity in the network (Login), stamp, electronic mail address or digital signature.

502. <sup>di</sup> “Article 7. Actions related to Information Security and Communications in the Ministry of Health will be guided by the following principles: (...) VI – Auditing and Conformity: a) the use of Information and Communication Technology provided by the Ministry of Health is subject to monitoring and auditing, as predicted in item 9.1.4 of the judgement of the Court of Audit of the Union no. 461 of April 28 of 2004, which provides for the regular analysis of log files with the use of, whenever possible, utilitarian software specific for monitoring the use of the systems, and, whenever possible, mechanisms that allow the traceability of this use will be implemented and kept; and

<sup>dii</sup> Article 13. This policy applies both to the computerized environment and to conventional means of information processing, communication and storage and is governed by the following guidelines:

XIII – Cloud Computing: a) the environment of cloud computing, its infrastructure and communication channel must adhere to the guidelines and norms of the Citizen Information Service of the Ministry of Health, and to current legislation; b) the contract for service provision, when applicable, must include clauses that assure the availability, integrity, confidentiality and authenticity of the information hosted in the cloud, especially those under custody of and managed by the service provider; and c) the storage of information in the cloud must be supported by a contract between the Ministry of Health and the cloud service provider, as to assure the availability, integrity, confidentiality and authenticity of the information hosted in the cloud (...).”



- 
503. <sup>diii</sup> Available at: <http://www.anatel.gov.br/institucional/ultimas-noticiass/2-uncategorised/1485-drones-devem-ser-homologados-para-evitar-interferencias>
504. <sup>div</sup> Available at: [http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00/@@display-file/arquivo\\_norma/RBACE94EMD00.pdf](http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00/@@display-file/arquivo_norma/RBACE94EMD00.pdf)
505. <sup>dv</sup> This distance may be negotiable with the consent of the owner of the building or facility.
506. <sup>dvi</sup> Exception made for cases in which ‘there is a mechanical barrier strong enough to isolate and protect persons who are not involved with the activity in case of an eventual accident’.
507. <sup>dvir</sup> This provision does not apply to the Public Power.
508. <sup>dviii</sup> Exception made for drones owned by entities controlled by the State.
509. <sup>dix</sup> The prohibition of autonomous operations does not imply a fence for totally automated flights, which are allowed, provided there is a possibility of intervention from the remote pilot at any time.
510. <sup>dx</sup> DECEA is the Aeronautic Command’s body for ‘planning, managing and controlling activities related to airspace control, flight protection, search and rescue services and telecommunications of the Aeronautic Command’. Available at: <http://www.decea.gov.br/drone/>
511. <sup>dxii</sup> DECEA, on its institutional website, has a simple example of how important it is for drone operators to observe the rules for airspace use: The drone operator wants to perform a flight over an uninhabited area of up to 400ft AGL (approximately 120 meters high). ICA 100-4, which deals with helicopter operations, determines that the minimum height for helicopter flights over uninhabited areas is of 200ft (approximately 60 meters). By this example alone, it is easy to realize that uncoordinated drone flights can cause conflict in case of helicopter traffic converging with the flight area, putting the helicopter at risk. Available at: <http://www.decea.gov.br/drone/>. Accessed on 10.01.2017.
512. <sup>dxiii</sup> Available at: <http://publicacoes.decea.gov.br/?i=publicacao&cid=4510>
513. <sup>dxiiii</sup> If used for specific activities such as aerobatics, compliance with norms of the Ministry of Defense is also required: <http://www.defesa.gov.br/index.php/cartografia-e-aerolevantamento-claten/legislacao-relacionada>
514. <sup>dxiv</sup> Law no. 7.802, of July 11 of 1989, regulated by Decree no. 4.074, of January 04 of 2002.
515. <sup>dxv</sup> Some examples are: Criminal Code – articles 132 and 261; Brazilian Aeronautic Code – articles 289 and 291; Civil Code – article 186; Law of Criminal Infractions – articles 33 and 35.
516. <sup>dxvi</sup> Response to contribution no. 19 in the public hearing on the regulation: “The autonomous flight is defined as the flight in which the remote pilot has no capacity of intervening in the aircraft’s operation during the flight. A totally automated flight with a pre-established route is not prohibited, provided that the remote pilot has the possibility of intervening (and supervising the entire flight) if needed”. Available at:
517. [http://www.anac.gov.br/participacao-social/audiencias-e-consultas-publicas/audiencias/2015/aud13/RAC\\_13\\_2015.pdf](http://www.anac.gov.br/participacao-social/audiencias-e-consultas-publicas/audiencias/2015/aud13/RAC_13_2015.pdf). Accessed on: 09.22.2017.
518. <sup>dxvii</sup> In this context, see ANAC’s response to contribution no. 229 of the public hearing on the new regulation: “(.) The instituted regulation was designed to be dynamic, constantly revised according to the emergence of new technological innovations in order to remain current, which does not prevent any specific user from requesting to ANAC a rule that is not yet permitted, under the form of exemption to compliance with the rules of RBAC no.11”. Available at: [http://www.anac.gov.br/participacao-social/audiencias-e-consultas-publicas/audiencias/2015/aud13/RAC\\_13\\_2015.pdf](http://www.anac.gov.br/participacao-social/audiencias-e-consultas-publicas/audiencias/2015/aud13/RAC_13_2015.pdf). Accessed on: 09.22.2017.
519. <sup>dxviii</sup> Public consultation conducted by Special Committee on Data Protection on July 11, 2017. The slides of the presentation are available at: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes->

---

[temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-publicas/sut.apres.audinciapblicaAP.11jul2017.pdf](https://www.camara.gov.br/legislacao/temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-publicas/sut.apres.audinciapblicaAP.11jul2017.pdf)

520. <sup>dxix</sup>Ibid
521. <sup>dxix</sup>Privacy and Security Principles for Farm Data. Available at: <https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data>. Accessed on 09.04.2017.
522. <sup>dxix</sup>Committee of Professional Agricultural Organizations (COPA) e General Committee for Agricultural Cooperation in the European Union (COGECA)
523. <sup>dxix</sup>COPA; COGECA. Main Principles Underpinning the Collection, Use and Exchange of Agricultural Data, no QJ (16)2689:6 – DA/FG/mvs. Brussels: Farmers European Agri - Cooperatives, [S.d.]. Available at: [https://ec.europa.eu/futurium/en/system/files/ged/main\\_principles\\_underpinning\\_the\\_collection\\_use\\_and\\_exchange\\_of\\_agricultural\\_data.pdf](https://ec.europa.eu/futurium/en/system/files/ged/main_principles_underpinning_the_collection_use_and_exchange_of_agricultural_data.pdf).
524. <sup>dxix</sup>Contribution sent by ABRASEM to the Personal Data Handling and Protection Special Committee (Bill no. 4.060/2012). Available at: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/ABRASEM.pdf>.
525. <sup>dxix</sup>It is important to note that the current definition of personal data provided by the Regulatory Decree of the Internet Framework already includes data that does not identify or may not identify a private individual (article 14, I of Decree no. 8.771/16).
526. <sup>dxix</sup>SILVA, A. P. *et al.* Um Novo Mundo de Dados - Relatório Final. Grupo de Ensino em Pesquisa e Inovação (GEPI-FGV). 2017. Available at:
527. [http://direitosp.fgv.br/sites/direitosp.fgv.br/files/arquivos/unmd\\_relatorio\\_fgv.pdf](http://direitosp.fgv.br/sites/direitosp.fgv.br/files/arquivos/unmd_relatorio_fgv.pdf). Accessed on 09.06.2017.