# ***WORLD LEGAL SUMMIT*** *– Belo Horizonte Session Report*


Image Credits: *World Legal Summit*

## *Introduction*

The *World Legal Summit* is an international initiative designed to enable the proposal of parameters for the creation of legislation for technology in a global scale, that occurred simultaneously in more than 30 (thirty) cities of 23 (twenty three) different countries, in August 1st, 2019.

Legal Experts, Entrepreneurs, Investors Public Power Representatives (Judiciary, Legislative and Executive), Academics, Technology experts and Lawyers were invited to participate, objecting to debate necessities, challenges and information and suggestions regarding four topics: (i) Autonomous Machines, (ii) Digital Identity & Governance; (iii) Cyber Security & Personal Data; and (iv) Startups Legal Framework, the latter discussed locally only.

Activities were conducted through panels with the participation of experts in each topic, with subsequent reunion of suggestions and deliberation of each topic in Round Tables (short design sprints). In view of those suggestions, we have prepared and hereby present this Report, hoping to enable the global compilation of efforts and suggestions with regard to the topics discussed.

## *Methodology*

As per the introduction herein, we hereby present the participants, panelists, panel mediators, round table coordinators, round table participants and staff that enabled the WLS Belo Horizonte Session and Suggestions:

**WLS LATAM Ambassador and Host of WLS Belo Horizonte Session: Paula Figueiredo**, lawyer, Founder of Figueiredo.law, President of Committee on Law for Startups – Brazilian Bar Association, Minas Gerais State Session.

**1st Panel: Autonomous Machines**

Panelists: **Dr. Rômulo Valentini** (Professor, PhD – Law and Informatics, Federal University of Minas Gerais – UFMG);

**Dr. Roberto Francisco** (CEO, Kukac – IBM Partner for AI for over 25 years)

Panel Mediator: **Ms. Lorena Lage** – Director of Academy Affairs of the Committee on Law for Startups – Brazilian Bar Association, Minas Gerais State Session.

**2nd Panel: Digital Identity & Governance**

Panelists: **Dra. Tatiana Revoredo** (CSO – The Global Strategy. Liaison do European Law Observatory. Founding member of Oxford Blokchain Foundation. Blockchain Strategist by Oxford University and MIT);

**Dr. Renato Martini** (Information Security Specialist. Technology advisor of the Federal Counsil of Brazilian Notary Board. Former member of the National Internet Supervision Board and Information Security Board of the Presidency of the Republic)

Panel Mediator: **Paula Figueiredo, President** of the Committee on Law for Startups – Brazilian Bar Association, Minas Gerais State Session.

**3rd Panel: Cyber Security & Personal Data**

Panelists: **Ms. Diego Machado** (Master of Laws and ongoin Doctorate in Civil Law by Rio de Janeiro State University – UERJ. Lawyer and Teacher)

**Sr. Johan Badra** (Senior Business Developer, Beijaflore)

Panel Mediator: **Sr. Bernardo Grossi**, President of the Committee on Data Protection – Brazilian Bar Association, Minas Gerais State Session

**4th Painel: Startups Legal Framework (Brazil)**

Panelists: **Sr. Sérgio Alves** (General Coordinator of Innovative Enterpreneurship of the Ministry of Cience, Technology, Innovation and Communications. Master of Laws, Berkley)

**Sr. Gabriel Ferraz** (Coordinator of the Legislative Affairs of the Public Policy unity at Brazilian Support Service for Small-sized companies)

Panel Mediator: **Luiza Patusco** – Secretary General of the Committee on Law for Startups – Brazilian Bar Association, Minas Gerais State Session.

**Round-table coordinators (design-sprint coordinators):**

Table 1: Caio Augusto Souza Lara
Table 2: Franco Maziero
Table 3: Júlio César Rodrigues da Silva
Table 4: Robert Emmanuel de Oliveira
Table 5: Isabela Magalhães Rosas
Table 6: Lucas Zauli
Table 7: Karina Coutinho
Table 8: Gustavo Babo
Table 9: Matheus Felipe Sales Santos
Table 10: Patrícia Garro

**Round-table participants:**

Adriano Ferraz
Alexandre Infante
Ana Flávia de Souza
Ana Lídia Figueiredo de Araújo Castro
Andréa Dombrowski
Bernardo Grossi
Breno Oliveira
Carlos Eduardo Rodrigues
Celina Rolim Reis
Ciro Chagas
Dario de Faria Tavares Neto
David Carvalho

Delvan Barcelos Junior

Eduardo Pinheiro Duarte

Felipe Moreira

Fernanda Horta

Fischer Stefan

Glaucia Silva

Guilherme Cekieira

Guilherme Di Buccio

Gustavo Babo

Henry Gabriel Colombi Barbosa Ferreira

Ivens Leão

Jeroen van de Graaf

João Henrique Kühl Bicalho

Karina Coutinho

Leon Spranger

Lindamaria Grasselli

Lívia Gamboge

Lucas Sávio Oliveira da Silva

Luciana Quaresma Rodrigues

Marcelo Pádua Cavalcanti

Marcus Drumond

Maria Flavia Maximo

Marianna Keller Lima Coelho

Matheus Queiroz

Natalia Tsuyama Cócolo

Pâmela Côrtes

Patricia Guercio Teixeira Delage

Paula Coelho

Paula Rocha Gouvea Brener

Pedro Henrique Esteves Freitas

Priscila Profiro

Rafael Guimarães

Rafaela Lauria silva

Rafhael Camargo

Renato Andrade

Robert Dannenberg

Rodrigo Pinheiro

Samantha Morais Nunes

Silvia Vanessa Rigatti Scherer

Thaís Delfino

Tiago Mol Arreguy Ferreira

Vanessa Emanuela Marques de Paula

Vinicius Miranda

**Staff:**

**Raphael Dantas:** Staff Coordinator and Rapporteur of the WLS Belo Horizonte Session Report.

**Germana Barros:** Event infrastructure Coordinator, Finance.

**Angélica Soares:** Participants guidance

**Bruna Carolina Silva:** Participants guidance

**Raquel Fernandes:** Participants guidance

**Lorraine Acipreste:** Director of media affairs - Committee on Law for Startups – Brazilian Bar Association, Minas Gerais State Session

**Leonardo Sahtler:** Design and Media specialist

Image Credits: Crypto ID

# *PANEL 1 – AUTONOMOUS MACHINES*

## *1) Necessities*

The first necessity identified in several tables was the creation of regulation of initial and preventive guidelines to deal with the issue based on the assumption that the legal system must follow this evolution / reality creating principles and logic exclusively for this regulation, as humans being the decision makers about the law. However, it would also be necessary to discuss the efficiency or inefficiency of technological oligopolies to measure how much regulation is needed and how it will be originated.

Legislation itself would address what is assured to humans rather than focusing directly on limiting Artificial Intelligence (A.I.). Still, legislation has to facilitate innovation, not to make it more difficult. Therefore, it would be applied by segments: (i) since the beginning of the process of innovation of Autonomous Machines such as, for example, regulating the ethics of the machine production ("how to produce"); (ii) define the degree of autonomy of Artificial Intelligence; (iii) the regulation of machine-human symbiosis as in the case of machines linked to humans (called Metahumans) or linked to the exercise of human work; (iv) the definition of criminal / civil liability (and degrees of guilt) with objective or jointly

agreed requirements for imputing liability and sanctions. For example, in the case of accidents involving autonomous cars or drones that cause harm to people; and (v) even the creation of "Permitted Risk" at the criminal level to provide legal certainty and attract programmers.

Regarding the principles, Transparency and Accountability were indicated as essential pillars in the creation of regulation by allowing: the auditing of codes (checking the coding quality of the algorithms - by Transparency by design or even via Blockchain), the compliance of protocols, the automation monitoring, reviewing actions of Autonomous Machines to generate control and limiting decisions made by Artificial Intelligence. In addition to the need to define civil and criminal liability to generate security and reduce risks from the concepts of A.I. also stipulated in the legislation.

From a human perspective, training and education at all social levels about the technological development translated by Autonomous Machines and Artificial Intelligence is fundamental, especially at the university level regarding technology courses, along with a kind of signature of terms such as a "Code of Ethics". Therefore, it is necessary to know the "unknown" in order to regulate it, to understand it and understand why a machine makes a certain decision in situations in which it is inserted and to address Ethics in all its logistics.

The regulation should try to answer questions related to liability in case of accidents and incidents with the A.I. such as: Is the responsibility of who acquired or of who consumed the object of the A.I.? From the manufacturer? From state / county legislating? From companies that map sensors used by Autonomous Machines? Objective or Subjective Responsibility?

Thus, there was an indication in some tables for the Guidelines Regulation to be created by an Independent Transnational Regulatory Agency formed by: specific academies, technicians (and related technologies), politicians representing the Governments of each country involved, professionals with expertise who are affected with such technology in everyday life. In other words,

the various sectors of society on an international scale as stakeholders in this process of creation.

In addition, it was suggested that the legislation should comply with EU regulatory initiatives, in particular two related to the development of smart robots: (i) the adoption of a mandatory registration of robots; and (ii) the creation of insurance that can cover the chances of damage caused by them.

## *2) Challenges*

A common perceived challenge was: How can we ensure non-corruption of A.I. even through the creation of a regulatory body and how would the collaboration in the process of creation of this body by the countries be? In this sense, the challenge is anchored in the following premise: creating global digital legislation does not imply the automatic and compulsory adherence of any country to this regulation, because the discussion to create the body would not only be anchored in the regulation, but also in the principles that govern it.

Therefore, the challenge would be to achieve global cooperation in a homogeneous manner on aspects of Ethics and unimaginable, yet possible, situations concerning Artificial Intelligence. Given that each country in its respective autonomy / sovereignty has different social, economic and cultural backgrounds, their needs and prerogatives are translated into heterogeneous notions about justice, reliability, privacy, security, inclusion, transparency and accountability. There is no guarantee of faithful adherence to the regulation to be proposed, nor a guarantee of consensus among all the international actors involved in each regulatory issue due to the discursive divergence about Ethics, besides the conceptual discussion of A.I. and its applications.

Also regarding the creation of this body, we highlight the limitation on the scope of global legislation to be applied to domestic levels and their sub-layers, the limitation in which regards the Public-Private spheres and also on how quickly

such legislation would be imposed and applied. Therefore, there would be no uniformity in the form of regulation nor in its application, disregarding the purpose of the creation of the organ.

Another challenge raised at the tables was the impact that the Guidelines Regulation would have on labor law and the impact on the transition of economic models by Autonomous Machines and A.I. evident growth (or based on geometric growth prospected by market experts). The relationship between human and machine generates changes in the forms and formats of work, which in turn would generate changes from the legal perspective of this subject.

There is an impact even when humans combine with machines (Metahumans) and this combination may suggest elevating the machine to civil status, as well as questioning the objectivity and subjectivity of human guilt in the decision-making process.

In this regard, it was also stressed the impact that regulation would have on criminal law, for example when A.I. causes fatal errors. It would require a profound alteration of this matter of law at the domestic level of each country, which suggests barriers to the conflict of national autonomy against different mindsets to reach consensus. To illustrate this challenge: it is unlikely to identify a technology developer's deceit, for if there is no action on the omission of a human being, there is no way to sanction or discuss the penalty applied to a machine / robot in a broad sense, so to speak. Or even the discussion about breaking the confidentiality protection of people in a particular place when a crime involving Artificial Intelligence occurs.

In all of the previous challenges raised it has also been paid attention to the issue of patents in technological systems, leading to the following problem: how would the boundary between patent (industrial secrecy / intellectual property) and the public interest be regulated in the face of data transparency and process operation and the A.I. decision making in Autonomous Machines? This suggests the possibility of data leakage in the broad sense and consequently

the disbelief in the systems, followed by the devaluation of the technological product and its regulation.

In addition, the challenge of implying that technology itself must be regulated by other technologies has been highlighted, which generates ambiguous and questionable reliability reasoning. Regulating technologies by other technologies involved does not guarantee corruption of both.

Finally, there was consensus on the notion that the challenges of creating specific regulations would slow the development of these technologies, either as a result of the bureaucratization process, the barrier of international collaboration or even inefficient applicability in practice by unmeasured variables. Regulation would be accompanied by setbacks.

## *3) Extra Insights*

The needs and challenges raised by the groups included final considerations and / or additional contributions on the topics below.

Regarding the creation of specific legislation, it was questioned whether it is possible to legislate before innovating or even if there is a need for regulation since some countries already regulate the sector in which the issue is involved, as in the USA. The United Kingdom and the European Union also act as regulatory agencies in setting development guidelines.

Still, thinking internationally about regulation, it was observed that its reflection may be interesting. However, if there is urgency at the national level and if any legislation can be discussed only nationally, it is rational and ethical to think about the obligation of a chair for discussion in the academy and the proper / local legal system.

It was considered that the focus is too much anchored on punishment processes when efforts should be allocated into thinking in collaborative processes to at least generate prevention. One way to achieve this could be by improving discriminatory algorithms, for example.

Finally, the importance of international law in regulating the major issues related to technological development in the attempt to create uniform legislation was also highlighted; in contrast to the barrier of regulating without curbing innovation.

Image Credits: Inforum365

## *PANEL 2 – IDENTITY & PERSONAL GOVERNANCE*

### *1) Necessities*

The suggestions arising from the second panel were rather homogeneous regarding some Challenges about the Digital Identity (I.D.) theme, from the national perspective.

The following stood out: (i) Through Public Policies, Brazil needs to create a State and Standardized Integrated System of Digital Identity, for both Individuals, Legal Entities and related. Given that Brazil spends more than BRL 7 billion per year in the process of issuing 7 (seven) digitized documents, the process could be compiled into just one unified digital document (if promoting such digitization could be considered feasible).

Taking into account such Integrated System (or Unified Database as also suggested), the organizational arrangement would bring benefits to digital citizenship by increasing the rendering of public digital services by the

government, as in the example mentioned at the tables: Notary publics can gain more agility while generating savings by the usage of unified digital documents. Resources such as digital traffic and cross-checking data tools in notary offices would ensure greater transparency and efficiency. It would also enable greater state investigative capacity by tracking identification technologies to point out fraud or combating corruption and money laundering. In addition, simplified systemic unification suggests improvement in public management as it enables diminishing of bureaucracy resulting from this process of digitalization.

Another aspect arising from the discussions would be the need to (ii) define the concept of Digital Identity (strictly for Identification and / or broadly for other verifications), as well as to define which unified data should be open worldwide, thinking globally, of those that should be of national open access only, defining also what would be of public access from what would be of private access to the citizen, in its uses and purposes.

Given the relevance of Cybersecurity on a federal scale, it is necessary to assign legal value to Data that has already been unified and also to stipulate the relevance of legal value applicability to other Data in demand for digital unification. Increasing security in this area was pointed out in the need to create manners of control and prevention of digital identity and data leakage, for instance as per the suggestion given at one of the tables: the use of blockchain network regulation as a standard of information security for personal data databases.

And, finally, the need to (iii) use this technology to improve infrastructure prior to or concurrently with the use of Digital IDs, also to combat corruption in public agencies regarding the cloning of identification records (“inside fraud”), as it highlights a national security problem.

## 2) Challenges

Numerous challenges were highlighted regarding the Digital Identity theme. Aiming at parallel yet connected spectra of analysis, the challenges permeate various spheres of the political, social, cultural and security environment.

There is a lack of interest at the political / federal level to unify data in a single document, for one or more reasons. The tables were systematically aligned in that matter: the difficulty of publicly certifying certificates and / or personal documents also extends to their digitization process; the publicity of public agents' salaries would be more evident after the digital unification of government systems, the non-adherence of notaries in the digitization process and the disorganized data between public agencies.

Assuming that Brazil is not 100% digitally connected, even in the fact that 10% of Brazilians do not have birth certificates, it was indicated as challenging to think about spending public resources on digital social security number process in a country that still needs to allocate efforts to its democratization process in pillar sectors inherent to its infrastructure. Thus, the perceived challenge for Brazil from the public and social point of view requires prior compliance with other actions in order to one be able to think effectively on the need and systematization of a unified digitization of certain documents to create Digital Identity.

From a digital security perspective, the challenge is compounded by the possibility of: data leakage, D.I. theft, identity fraud, digital certificate forgery, and other known digital corruption present in data traffic. There is sensitivity in data protection because there is technological vulnerability in the Government. Even the General Data Protection Act (Brazil) was consider a challenge itself. In short, there is no gap necessarily in a regulation, but there is a gap in the institutional effectiveness by the State in unifying and protecting these data.

The challenge also transforms itself and shifts into the cultural sphere of social (or ethical) education: educating data accessibility for individuals and promoting digital literacy / digital inclusion are tasks that require time and public funding for education campaigns that raise awareness and foster useful public knowledge. It was also emphasized that Brazilians tend to be conservative and dependent on pre-existing binding norms to adhere to new forms of use and consumption when it comes to the public sphere.

Another perspective of reasoning also questioned the role of Government in the application of these data and the proposed challenge is anchored in the sensitivity to social freedoms. The problem is: how to align the principles of Transparency, Privacy, Property and Security among public agencies in the face of the true consent of society regarding the way the Government applies its data. That is, what data will be required to be collected for digital unification without harming rights such as the right to anonymity of identification and data, for example.

In addition, the challenge was intensified by thinking about the right concept of Digital Identity to be adopted (as well as the concept of Ideological Falsehood) by the body of regulation. Thus, the challenge was translated into the following: which determination should be used for deciding which personal data to be collected for unification and also which analysis would this be based to measure usability / utilization / attribution of this data. In view of the transparency: who will have access to the data and what kind of data it will be?

## *3) Extra Insights*

The extra insights on Digital Identity were rather balanced, even though the discussions on this regard is not fully consolidated in Brazil. Participants pointed out that it is interesting to consider overcoming barriers of reliability and security in the public system or even in the process of universal digitization to establish digital democracy. Considering that the end user (the citizen / individual)

will have some control of their own data, the security instinct related to such control data might be sharpened or even incline the individual to reason that their freedom and right to anonymity must be preserved, especially in view of the principles of Transparency, Security, Property and Privacy.

In one of the tables, Estonia's example (a country located on the eastern Baltic Sea coast of northern Europe) was mentioned: Estonia is the world's greatest benchmarking for reducing bureaucratic processes: the digital identification system is mandatory for citizens and offers several solutions using a same card. The country has overcome the barriers of reliability and security to establish digital democracy. For instance, it is possible to complete the sale and transfer of a vehicle in the country in a 15 (fifteen) minute process.

Therefore, the Government could, despite the challenges highlighted, implement unification of Digital Identity by segmenting data by purpose and relevance, along with strong data protection action, as was done in Estonia, but given the avoidance of excessive social control, preventing abuses and excesses of State control over Data. Another important suggestion that arose was the inclusion of refugees and stateless persons in digital identification systems in order to ensure access by this population to public and private services.

The Chinese project referred as Social Credit System was cited in discussions, which purpose is to gather of financial information, online activities such as: sending messages, websites accessed, tweets, publications and sharing of images and videos, as well as criminal records of each individual, all on one digital card. Criticism regarding the project is based on the premise that this would increase the surveillance power of the Chinese government by giving authorities a mass analysis tool. Thus, the concern is that the project could translate into vulnerability, either from the perspective of the individual towards society and government, or from the perspective of the Federal / National before other countries of the International System.

Finally, regarding the public sphere and its relation to the private environment, there were two prominent considerations. The first relies on the

logistics that the creation of I.D. could allow greater interactivity between the individual and the Government, in order to generate personalization of digital public services based on this user's data.

On the other hand, the risks of the Digital Identity process were again considered. Unified information would become an object of desire oft private enterprises to seek access to information essential to implement a robust marketing system that generates competitive advantage in the marketplace. From this perspective, the possibility of system corruption and consequent data leakage was also attributed as risk observation.

Image Credits: Jusbrasil

# PANEL 3 – CYBER SECURITY & PERSONAL DATA

## *1) Necessities*

In compiling the tables suggestions for the third panel, the identified necessities converged on technical, legal / political, cultural (from the point of view of governance practices within the business ecosystem) and social developments. Law 13.709/13, better known as the General Personal Data Protection Act (LGPD) was, in addition to cited in all Sprints, also used as a reference and basis for expressing changing needs in the Legal, Technical and Corporate fields.

In short, from 2020 onwards, any person and company, whether public or private, will need to adapt their personal data collection, use and transfer processes in Brazil to a scope of rules governing the handling of any data. information that can identify a person. In short, explicit consent will need to be obtained and customer / user data protected when collecting, storing and using this information. The law aims to increase the data subject's control over the

information, bring transparency and legal certainty to public and private sector entities.

Recently, in July 2019, the law establishing the National Data Protection Authority (ANPD) was approved, a public administration body that will be the entity responsible for the supervision and adoption of good practices (appropriate practices) for the collection and processing of personal data by entities and persons. Therefore, its creation was considered fundamental to ensure the effective application and compliance of the LGPD. This body will work like an ANATEL or PROCON, for example.

With this in mind, the groups recommended the following assumptions: (i) there is a need to establish and disseminate a Data Protection Culture to jurists, entrepreneurs, IT technicians, users and other stakeholders in the ecosystem through the dissemination of fundamentals, LGPD principles and sanctions.

The development and multiplication of this law-based mindset would be anchored in the convergence of integrated work between various sectors, including the recently created ANPD and other related legal entities. It was suggested the creation of an independent and multidisciplinary Security Committee that defines unique process standards, procedures and tools to harmonize data protection management by entities. The proposal would be to measure and implement these mechanisms to achieve compliance with the law guidelines.

Regarding the processes and tools, the following were mentioned: the possibility of audits or registration with the ANPD attesting to the company's suitability; the creation of diagnostics to assess the real need for data compliance and criteria; and the definition of Cyber Security internal processes as a deployment of Compliance aiming to generate a funnel to mitigate the possibilities of data leakage through continuous improvements. The goal here is information security, ie the ability to preserve the confidentiality (protection of privacy), integrity, availability and authenticity of information.

In addition, some supporting Principles for the creation of this multidisciplinary entity were also pointed out: (a) Privacy by Design, which is based on the premise of prevention and anticipation of events that may compromise data privacy before they occur, either from the process of designing IT systems, to business practices, projects, products or any other solution that involves the handling of personal data; (b) Also define Parameters to measure impacts of accidents and incidents with practices around personal data; (c) Encourage the Data Protection Culture through cooperation within, outside and between the entities and their respective professionals involved; and (d) encourage the collection of transparency in the processes of data collection, processing and use by entities

From the LGPD's legal perspective, it was pointed out the need to (ii) extend the liability of sanctions already provided for by law in the civil sphere by quantifying / pricing the value of the leakage of personal data that violates their privacy. Given that the predicted fine is punitive in nature, the focus should not only be on a financial penalty, but also on educational punishment, such as the paralyzing of the company's activities regarding the processing of data and the focus on the company's bad reputation, in addition to public retraction. It was also suggested the implementation of a whistleblower awarded the existence of data protection departments, as in a model similar to the Anti-Corruption Compliance Act.

These differentials that would make the law more effective and foster the Chain of Defense logic, in which large enterprises may require smaller companies such as partners, suppliers, and outsourcers to pay attention to their alignment and adherence to the law. At this point, the need was raised for LGPD to provide flexibility for small businesses, either by means of adaptation or even by the extension of vacatio legis, considered small for small and medium enterprises.

From the business point of view, the dissemination of the Data Protection Culture in the business territory required (iii) to make companies aware of the existence and encourage in-depth knowledge of the legislation, as well as being subject to LGPD. Understanding the law, the impacts and duties it imposes will

require compliance within companies, which can lead to: creation of training courses for IT professionals and other teams involved in data processing, reorganization of data use and storage, sustainable technological development thinking about Privacy by Design, promotion of related workshops in the private sphere, among others.

Finally, the issue of technique and the end user, the individual in whom the whole subject of personal data protection is anchored, was also mentioned. With respect to the Brazilian population, it was found necessary (iv) awareness of the need to protect user data and the ways in which this is done and protected by law. For example, such awareness was required upon the entry into force of the Consumer Protection Code.

In this sense, digital literacy would require understanding by the user of the value that their personal data have from a constitutional, financial and security perspective. For instance, this assumption is validated by the importance of protecting third-party data in judicial or administrative, physical or electronic proceedings in the Brazilian scenario, especially in relation to the political context, as has been seen in recent years.

In the context of digital literacy, it was also indicated the need to create Terms of Use and Services or Contracts to maximize fully informed consent, whereby users should be given access to information about the processing of their data and how and with whom (other entities) sharing is performed. Added to this paradigm, was thinking of the logic of User-friendly: term used to define a platform, program or application that is easy to use and with which it is possible to interact with the user, in its basic functionalities, intuitively, without recourse to manuals.

## 2) Challenges

Just as needs were well explored, challenges also went through a long critical scope to produce insights related to technical, legal / political, cultural and social formats.

Regarding corporate governance in data protection, the challenge revolves around the question of whether LGPD will be truly effective in the face of the sensitivity of education and dissemination of culture to this issue, both public and private. Many questions are still part of the discussions about LGPD, its adequacy and even about the operation of the supervisory body due to the volume of data to be supervised and the political forms and figures linked to the public agency.

It has been assumed that many companies (public and private) ignore legal legislative issues along their way even to be able to promote organic and strategic growth. In addition, it is thought that data protection and cyber security will be part of data governance by corporate culture only as far as punishments in law are concerned. Therefore, the dissemination of good practices arising from the promotion of culture as part of the development by adaptation and evolving necessity of the business market loses strength, when the focus is only punitive character for not adhering to the practices to predict risks of digital business. This leads to a lack of business perspective on the competitive advantage gains that compliance with the law will generate for the respective business models.

In addition, it was also worth considering the challenge from the cost-benefit perspective for these companies to implement the science of data protection in their respective internal governance. Given that training should be continuous thinking about the rotation of employees and public servants within a private or public company, this implies constant investment (or cost depending on the criterion used by the company) in the qualitative qualifications of the professional, being the full responsibility of the company to promote it. It also

implies the difficulty of implementing compliance with the law due to communication and mapping.

The question is whether there will be public and private confidence in the new data protection system. Yet, adequacy is most unlikely to apply this paradigm to small and micro enterprises.

Switching to user bias, challenges identified were the resistance of the individual to read terms of contracts and whether consent actually exists. Thinking about the educational adaptation to the data protection culture and its importance by users, Brazilians do not have the habit of reading everything they sign for consent, suggesting barriers even in the use of User-friendly application as an attempt to generate transparency and understanding of terms and the collection of personal data.

On technical, legal and political aspects the discussion turned to the figure of the National Data Protection Authority and some questions involved in the implementation process. The Brazilian Government repealed the part of the law that prevented private companies from being able to process public security, defense and even national and criminal data. This change in the law also unfolded to the political body, in which the situation of the “political” choice of the ANPD's board of authority and the absence of other appointments were questioned. The ANPD will have technical autonomy, but will be linked to the Presidency of the Republic. However, positions with low remuneration, in addition to lack of independence combined with political instability, are grounds for questioning the Authority's real independence and effectiveness, among other things.

In this context, challenges were posed regarding LGDP's relationship with the ANPD along the following lines: LGPD for public entities does not define the “social function” of personal data. The Government may use user data for the “shared processing and use of data necessary for the execution of public policies provided for in laws and regulations or supported by similar contracts, agreements or instruments” and “for compliance by the controller or legal or

regulatory obligation" without having to inform the holder about the use (information officially released by the National Agency).

Therefore, the effectiveness of the ANPD in overseeing the application of LGPD principles was questioned even by the lack of transparency in the Government's own use of personal data in light of the "social good". It is unlikely to stipulate specific regulations by the ANPD for specific markets, as there is no clarity in certain guidelines yet, for example, of the difference between misappropriation of data and cross-checking.

## *3) Extra Insights*

As it is considered a relatively new theme in Brazil, Data Protection and Cyber Security still has many debates ahead in time. However, some valid concluding remarks were highlighted at the tables.

Regarding LGPD's relationship with the recent ANPD, it will need to define clear parameters for the applicability of penalties, sanctions and also LGPD principles. In this regard, it was emphasized that the Government has a range of options to better develop its transparency and adherence to the law itself, as observations indicated: the creation of public policies aimed at allocating resources for training public agents; fostering cyber security investments; the Government to make data on the performance of public agents increasingly public.

As for the LGPD itself, it was considered important not only to relax sanctions for greater effectiveness and efficiency in their applicability, but it was considered that the law also encourages the generation of opportunities for new business models that address better understanding for processing data and so they can use the data more wisely in terms of technical, social, financial and legal context, achieving optimal results.

A final relevant consideration: the importance of encouraging studies on European experience in the implementation of the General Data Protection Regulation (GDPR) standards. Given that personal data is the new fuel that drives contemporary international society, this “new oil” should receive attention in all spheres that composes developed societies as well as those in development of the following structures: social, cultural, political / legal and financial with regard to private market and the relationships between personal data and cyber protection.