Centre for Information Policy Leadership (CIPL) and
Centro de Direito, Internet e Sociedade of Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS-IDP)

International Dialogue on LGPD Implementation in the context of Global Data Protection

19 and 20 May 2021

Opening Day One – Looking back six years and looking forward in data protection in Brazil and around the world

We are experiencing the fourth industrial revolution, and the COVID-19 pandemic boosted this movement of innovation. According to **BOJANA BELLAMY**, CIPL's President, two of the consequences of this are the increase of international flow of personal data and the development of Artificial Intelligence (AI) systems. The ability to use AI depends on accessing data, processing it, and having pools of information for relevant purposes. In this sense, in the last six years, we have been experiencing some tensions that must be analyzed: it is the age after the GDPR, which was a trend for many countries in terms of regulating the processing of personal information; free data streams, where governments are realizing the importance of data and using that information for economic and social purposes, at the same time there is concern about data transfer and sovereignty; finally, the responsible use of data, given the companies' boards responsibility concerning data.

LAURA SCHERTEL, CEDIS's Director, said that the year 2020 was decisive in Brazil. During this year, the Brazilian data protection law (LGPD) came into force, the new Brazilian data protection authority (ANPD) was established, and the Brazilian Supreme Court (STF) decided on the existence of a fundamental right to data protection. Therefore, we need to think about how to apply the LGPD to generate trust in the relationships between companies, data subjects and the State. Still, it is expected for the data to flow, so the debate must also be considered at the international level. In this sense, the partnership between CEDIS-IDP and CIPL is essential to help build an effective interpretation of LGPD, even considering the peculiarities of each country, such as the challenges of institutional regulation.

Keynote 1 - ANPD's regulatory agenda and priorities

WALDEMAR GONÇALVES ORTUNHO JR, Director-President of the Brazilian National Authority (ANPD), highlighted that it is essential to promote the theme of data protection in events, considering the recent creation of the ANPD and the challenges that the authority is currently facing. As a result, there is the necessity to stimulate a debate on how data protection affects the daily life for Brazilian citizens. Despite the challenges of starting an authority and still having a reduced staff of 36 people, the ANPD has already carried out relevant actions, such as publishing the internal rules of the authority[1] and a regulatory agenda[2] to ensure that processes are conducted in a timely manner. These measures were based on the analysis of experiences of other national and international agencies that mapped the procedures that could be adapted and replicated. Thus, it will be possible to build a stronger structure for the brazilian authority, considering that Brazil is a country extensive and peculiar. In addition, it will be necessary to organize plans, such as the possibility of reviewing the ANPD's internal organization. Another challenge is the qualification of staff, but this activity is already under development, especially considering the attendance of the staff of the ANPD in a specific course provided by the European Commission.

The President added that there is also the challenge of additional regulation, so a map of the topics was made, and the priorities of the Authority were defined to form a solid Regulatory Agenda. This does not mean that other agendas will not be faced by the ANPD, since the reality brings challenges that will be studied according to specific demands, such as the issue of international data transfer. The development of the regulation will occur through public hearings and the submission of contributions. This methodology is being followed in the case of the analysis of issues such as notification of security incidents, as well as distinguished approach for small and medium-sized companies. Another ANPD action was regarding the privacy policy of WhatsApp, in which the ANPD, in collaboration with other bodies, had the opportunity to present a note on the update of the privacy policy. Finally, it was emphasized that the ANPD believes that the priority is to create a culture of data protection, raise awareness among the population and highlight the functionality of good practices for companies, only then LGPD will be applied in a responsible and transparent way.

[1] Available in: < https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 >.
[2] Available in: < https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 >.

Keynote 2 – Global and UK perspectives on data protection

According to **SIMON MCDOUGALL**, Executive Director – Technology Policy and Innovation and Deputy Commissioner of the Information Commissioner's Office (ICO), data protection authorities were already facing several challenges in dealing with the implications of the data protection issue, but COVID-19 has accelerated the urgency of these challenges and presented new ones. Some examples of innovation were seen in the use of health data to speed up vaccination programs and decrease virus transmission as well as in the cases of vaccine passports and contact tracing applications. In this way, power imbalances were perceived in the context of privacy, but Simon pointed out that trust is a key distinguisher for citizens' data protection compliance.

It is now clear how data is embedded in our daily life, the amount of data produced is constantly increasing. With the COVID-19 pandemic, this statement becomes common sense, and other stakeholders have awakened to this issue. For data protection authorities, this means that the front line of work is broad regarding different issues that need to be addressed. Therefore, one should focus on defining priorities, since there is a difficulty in maintaining this agenda in the face of the new demands created every day. Furthermore, one must pay attention to risk management, with a multidisciplinary perspective in this complex scenario, and with access to knowledge beyond the law. It is also necessary to have solid principles, access to other actors, and awareness of the social context.

For ICO, privacy is a fundamental but not an absolute right, and COVID-19 made this clear. In this context, some challenges have been set on the impact of data processing regarding the privacy of society, so public trust must be maintained for citizens to feel comfortable. The authority will only be effective if it works together with regulators, legislators, and others social actors. This understanding resulted in the creation of the Digital Regulation Cooperation Forum (DRCF), in which competition, communication, and data protection began to work together. Thus, a joint work plan[3] was published so that there is consistency in regulating matters of collective interest in the United Kingdom.

[3] Available in: << https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122>.

Panel 1 - Regulation for results in data protection: cooperative engagement, effective oversight, smart enforcement

ARTHUR SABBAT, Director of the ANPD, believes that since the Brazilian authority is new the first activity was to set a specific regulatory agenda with ten actions for the ANPD. The topics were chosen for their potential impact on society and individuals in general, in addition to the benefits for the community and respect for their rights.

As stated by **ANNA MORGAN**, Deputy Commissioner of the Ireland Office of the Data Protection Commissioner, Ireland's authority is also setting priorities, and there is a challenge in defining which issues should be looked at since resources are limited. Balancing the interests and risks of data processing is a challenge when dealing with the demands of the society. Therefore, until May 2020, the authority analyzed cases that were reported; but, as a rule, the complaints were of an individual nature and related to labor or consumer areas. That is, they were not cases with a significant systemic or collective impact. At the same time, many issues must be addressed at a broader level than that indicated by GDPR, in addition to support for compliance projects undertaken by companies and thorough analysis on the volume of issues brought to the authority.

ZEE KIN YEONG, Assistant Chief Executive of the Singapore Personal Data Protection Commission, believes that Singapore's data protection law ensures the protection of consumers' personal data and allows businesses to have legitimate use of personal data. These two elements are the focus of the authority's work. For the Singapore authority, it is crucial to disseminate good practices. This strategy has been followed in the case of knowledge sharing with the Singapore Council, aimed at the private sector. This Council looks after companies and establishes guidelines for corporate organization so that data protection is respected by the companies' decision-making bodies. Therefore, the authority seeks to recognize companies that adopt relevant data protection practices through certificates. In this way, companies start to act with the support of the authority so that there is transparency but also protection of the companies' interests. This system organized by the data protection authority also supports the reputation of companies on privacy practices, creating effective incentives for large corporations to adopt good practices.

In the opinion of **GUILHERME ROSCHKE**, Counsel for International Consumer Protection at the Federal Trade Commission, a specific and current issue is the discriminatory bias of algorithms in the face of flawed tests and faulty inputs. The starting point for solving this issue is transparency and accountability; developers must ensure that decisions are

defensible and explicable, and it must be possible for third parties to test these systems. However, transparency cannot create unreasonable burdens for consumers, such as overly lengthy privacy policies. Also, in the case of facial recognition technology, there are studies on the difficulty of this technology working efficiently with non-white individuals, which presents a high risk. Another agenda is to protect youth data since the use of technologies for education has expanded significantly considering the COVID-19 pandemic.

Another tool used to solve investigations related to privacy violations is accountability, which is not only about negative financial consequences but also to mean an incentive to companies to adopt compliance practices for competitive and reputational advantages. Soon companies will realize that practices against data protection are not profitable and that it is relevant to have accountability measures to promote transparency measures for the protection of victims who have suffered damages, besides analyzing algorithm bias issues. Furthermore, this is determinant to establish clear and transparent rules to know what they are doing, and which practices are considered unfair.

It is also important to hold workshops to raise awareness of consumers and the civil society so that everyone knows and has experiences to understand how to act in concrete cases. This practice also helps in forming an understanding of the law and in defining what is allowed or not, to delimit situations that should be taken to court litigation. Another practice is cooperation, which is done through norms that allow the exchange of confidential information and the sharing of experience and know-how. All these measures are effective when carried out jointly so that the sectors know about the issues and promote behavioral change.

In the view of **CHRIS HODGES**, Oxford professor, there is a global trend for regulations to follow a risk-based approach. This movement must be followed by actions focused on substantial behavioral change in the relationship between companies and individuals. That is because, as a rule, the motivation for change is linked to the behavior of individuals and not necessarily to the regulatory and punitive responses provided by law. In small businesses, it is interesting to offer support so that they become more engaged in data protection issues, since sanctions could lead to the closure of these companies. Thus, the authorities have a role in communicating with key persons, such as company directors, to effectively influence behavior and add risk and outcome approaches to resource allocation. In addition, ethical regulations and codes of conduct are matters to be observed in companies to promote a culture of data protection.

EDUARDO BERTONI, representative and coordinator at Regional Office of the Inter-American Institute of Human Rights for South America (IIDH) and former Director of the

Agência Argentina de Acesso à Informação Pública, believes that one of the priorities of the Argentinian authority was to make it as independent as possible. Until 2016, the authority was linked to the Argentinian Ministry of Justice and Human Rights, and, therefore, the directors within the authority could be removed at the discretion of the Minister of Justice. Since then, the need for greater independence of the authority has been perceived, and, therefore, these issues have become the scope of the Access to Information Agency. Therefore, there was a joint effort for this independent and autonomous structure to be achieved. Moreover, the participation of the authority in international forums strengthens the independence and benefits the agency in law enforcement, as is the case of Convention 108 for cooperation in the investigation. In the case of Brazil, the LGPD should be implemented to ensure greater autonomy to the data protection authority (ANPD). Still, this topic gains greater relevance in the Mercosur debate, which should be strengthened in the future.

Panel 2 - The role of data privacy accountability: building risk-based data management programs and demonstrating compliance

The goal of this panel was to understand how companies implemented specific practices in the context of accountability and data protection. There is an increasing expectation from regulations that organizations must be accountable and have privacy policies and related good practices. This reality is followed by the trend of setting the business agenda of companies and the interests of privacy-focused corporate boards beyond legal compliance. In addition, the COVID-19 pandemic transformed accountability as an institutional compass for the post-COVID world.

In this perspective, **ROB SHERMAN**, Vice President and Deputy Chief Privacy Officer of Facebook, stressed the necessity of thinking about international practices for accountability and oversight since, nowadays, many companies serve consumers worldwide and must adapt to each legislation. Due to that, building a regulatory implementation approach that divides the implementation of the law into different focuses is a relevant movement. Moreover, the possibility to consult with the DPA on their expectations on compliance is crucial for making informed decisions. In some cases, this external consultation can have inputs from the academic and the civil society sector. Investing in security and developing risk assessments play an essential role in making the company accountable, and they help to maintain consistency and audibility over time.

In addition, **CAROLINE LOUVEAUX**, Chief Privacy Officer of Mastercard, agrees that a data protection culture starts at the highest level of an organization. In the context of accountability, the company implemented its binding paper trolls in Europe and achieved CBPR (Cross Border Privacy Rules Certification) certifications because they are tools that demonstrate that the business is compliant with the requirements of privacy. To illustrate compliance-related activities, **CAROLINE** pointed to implementing governance tools and mechanisms to ensure effective compliance, the network of privacy and data protection offices, and conducting audits of data practices. As a rule, **CAROLINE** believes it is more effective to have a single program of compliance based on the highest privacy standards and adjust from there rather than having multiple different programs decentralized. To conclude, the CPO affirmed the utility of having a specific policy to data breaches so people would understand what to do and how to act quickly. At last, she spoke about the awareness and training sector specialized conducted every year.

RENATO MONTEIRO, Twitter's Data Protection Counsel Lead for LATAM, described a movement toward understanding privacy as a corporate objective. Consequently, privacy and information security have become part of the company's career advancement parameters and any interested employee can take a privacy certification. Another practice is to keep an open dialogue with regulators about the process of reviewing privacy practices; this occurred with ICO, for example. Furthermore, Twitter indicates the legal basis for processing personal data and maintains the summaries of the legitimate interest assessment (LIA) publicly. The company retains the international privacy program at a global level, but increasingly regional approaches based on risks and benefits have been stablished.

According to **ROBERTO BRUCE**, Data Privacy Manager of Bradesco, accountability runs through all the entire data protection regulation. In this sense, the LGPD encourages the adoption of good practices by processing agents. To understand and apply the principle of accountability, the company decided to work with the Brazilian Federation of Banks (FEBRABAN) to adopt the most recommended paths, implement good practices, and produce informative videos and courses. Furthermore, the board appointed a data protection officer (DPO) and indicated the name and contact of the DPO on the bank's website in addition to creating means for data subjects to exercise their rights.

MARLON DOMINGUES, Erasmus University Rotterdam DPO, noted that in the case of local companies, for accountability, it is necessary to establish leadership to conduct the compliance program and develop privacy policies and other updated and specific standards. Another relevant aspect is to build a framework for the privacy program, because in the case

of organizations in the education sector, the company may be compliant in three levels: within the organization, in international collaborations and the higher education sector.

On the other hand, although the World Bank is an international organization, which is exempt from following any country-specific regulations such as the GDPR or the LGPD, the institution realizes the risks of ignoring issues regarding the use of personal data, specifically in research conducted by the bank. For **TAMI DOKKEN**, World Bank's Chief Data Privacy Officer, these risks include losses to legal business and hurting the bank's own reputation. The bank voluntarily implemented the first personal data privacy policy that went into effect in February 2021. Specifically on accountability, the Bank's privacy policy requires accountability both internally and externally, and the data privacy governance is used with the standard three lines of defense model in which all staff is responsible for integrating data privacy into their daily work. Moreover, the bank has conducted a risk assessment of every business unit region and practice group to identify the organization's activities that involve personal data and thus close any gaps that have been identified.

MARCOS OTTONI, the legal coordinator of CNSaúde, highlights that the health sector is called upon to adapt its internal policies, implement privacy guidelines, and use personal data to fight the pandemic rationally. Therefore, the organization noted the possibility of providing good practices at the individual level and in associations. Considering this, CNSaúde launched the Code of Good Practices for Private Providers in Health[4]. The establishment of this privacy policy between the organizations that compose CNSaúde serves both to protect the data subjects, guarantee commercial symmetries, and avoids competitive distortions. In the entity's opinion, the code of good practices will be since it is not a static text that does not observe concrete and new issues. Thus, it is essential to act alongside public authorities so that the problems are debated in a reasoned manner.

Opening Day Two

First, **GIOVANNA CARLONI** and **LAURA SCHERTEL** point out that the day's discussion will deal with international data transfer and data breaches. It should be noted that this discussion is closely linked to the topics of the previous day (regulatory models and accountability), since the procedures arising from these topics are essential both for the international transfer of data and for the dynamics of data breaches management.

[4] Available in: < http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/

Keynote 3 – Data Protection Officers and the rise of the data privacy profession around the globe

The first speaker was **TREVOR HUGHES,** CEO and President of the International Association of Privacy Professionals (IAPP), the world's largest community of data protection professionals. Trevor brings up the fact that the professionalization of those involved in data processing is central to effective data protection, and that the GDPR has emphasized this need. In Brazil, for example, it is estimated that 50,000 professionals will be needed in the area. In this context, a well-trained professional is essential, adding great value to data protection and the digital economy. Thus, he explains that the main function of the IAPP is precisely to create mechanisms, such as training and the increase of higher education courses in the area, in order to train DPOs and other professionals that work with protection of data.

Keynote 4 – Creating a pro-growth and trusted data regime under the UK's National Data Strategy

After Trevor, it was the turn of **JAMES SNOOK,** Director of Data Policy at the UK's Department for Digital, Culture, Media and Sport (DCMS), where his main function is the development of data protection regulations. In the presentation, he dealt mainly with the UK's National Data Strategy, published in 2020. The importance of the document was justified on three grounds: (i) the economic value of data in modern times; (ii) the value of such assets to public institutions to improve their efficiency; and (iii) the risks arising from data processing to individual rights.

Thus, it is understood that the main objective of the Strategy consists in minimizing the risks and maximizing the opportunities arising from new technologies and data processing. To this end, he separated the intent of the National Strategy into five missions:

(i) to ensure an environment where the economic value of data can be thoroughly exploited;

(ii) create a pro-growth environment that considers the limitations of each organization to define its data protection obligations;

(iii) maximizing public efficiency in the performance of their services through data processing;

(iv) establishing a strong risk management framework, in light of our increasing dependence on technology and data processing; and

(v) creating a strong legal and regulatory framework for establishing a secure environment for international data transfer, placing the UK as an international leader for the development of this pillar.

Panel 3 – Enabling international data transfers across regions

The first panelist was **MIRIAM WIMMER,** director of the Brazilian Data Protection Authority - ANPD. **MIRIAM** spoke about the fact that data protection is an incipient subject in Brazil, which makes the discussions move at a slower pace. Even so, she said that the ANPD is setting priorities for the development of the subject in Brazil, among them, the cross-border flow of data, which has regulatory space planned for the first half of 2022, according to the regulatory agenda published by the Authority. In this context, **MIRIAM** closed her presentation stating that the initial scope will be a regulation focused on the practice of data transfer in the daily life of companies, the most straightforward and urgent issue.

The next speaker was **YUJI ASAI** of the Japanese Data Protection Authority. He addressed the mutual recognition between Japan and the European Union for the free flow of data, stating that this is achieved through trust, which is built on similar data protection structures, regardless of cultural differences between countries or regions. Lastly, he explained the existence of certificates that allow the free flow of data, which attests to the trust between countries, and which may serve Brazil in the future.

The third speaker was **JOE JONES,** also from the UK's Department for Digital, Culture, Media and Sport (DCMS). The speaker also mentioned the need for a culture of data protection, which varies from country to country depending on their background. In this regard, he pointed out that to establish mutual adequacy for the free flow of data, there is no need for correspondence in the regulations themselves, but there is a need for identity in the data protection framework and in the general principles that guide it. In addition, he stressed that the adequacy process must take place with a sense of mutuality and a cooperative spirit, not with one country or region providing rules that the other must accept. The agreement with Japan is an example in this sense, as it was conducted with much dialog.

Following this, **KATE CHARLET,** Google, addressed the audience. The speaker began by mentioning the importance of global computing. According to her, the interconnected network around the globe helps in information security, assisting, for example, in mapping the flow of data in a system. With this it is demonstrated that a global free flow does not mean a

necessary threat to privacy. Furthermore, **KATE** highlighted the importance of the free flow of data for society, going from the advantages that all companies find when there are no barriers to this flow to the benefits that this has for the consumer's life. Finally, she emphasizes that such liberty is not paradoxical with data protection, and that both must adapt and subsist.

The fifth speaker was **JACOBO ESQUENAZI,** from HP. The big question debated by the executive concerned the certificates of trust issued by some countries for companies. **JACOBO** affirmed that this is an excellent instrument for compliance with the strictest data protection and transfer standards, since, for a global compliance, the company will have to use a code of conduct that is adapted to the rules of the regions where it operates. He pointed out that one of the main difficulties for countries to build their certificates is the lack of a critical body to rule on cases. He finally advised Brazil to approve or recognize the certificates that already exist.

The last speaker in the panel was **MARCEL LEONARDI,** partner at Leonardi Advogados. He presented the issue arising from the absence of mechanisms for international data transfers in the Brazilian regulatory context, in view of the incessant need for companies to carry out cross-border data processing operations. Between following the European legislation for data transfer and other possibilities, **MARCEL** pointed out that the best alternative is for companies to establish an intense debate with the ANPD so that it may provide the guidelines for the international flow of data while there are no solid regulations or other instruments on the subject.

Panel 4 – Reporting and managing data breaches and notifications: a challenge for both organizations and DPAs

The first speaker was **JOACIL BASÍLIO RAEL,** Director of ANPD. The panelist emphasized the seriousness that data breaches can have, especially when they involve sensitive data, generating irreversible individual and collective damage. He stated that, with this context in mind, the ANPD adopted as a priority the regulation of data breaches and its notification, and that, as early as 2021, a Call for Proposals was launched by the Authority, in order to provide guidance to civil society, what will lead to complementary normatives.

The next speaker was **DAVID STEVENS,** from the Belgian Data Protection Authority. Based on Belgium's experience after the GDPR came into force, David stated that it is common for data breach notifications to increase once the data protection regulation is in place. In this regard, he pointed out the importance of certain measures, such as (i) having good

organizational standards, for instance through the implementation of software that separate and organize incoming notifications, (ii) being able to select and give more attention to what is important and has learning potential, and (iii) communicating to society about data breaches with caution, providing only the right information about the case, without a lot of fuss.

Next, **BRIDGET TREACY,** partner at Hunton Andrews Kurth, addressed the audience. The speaker pointed out that data breaches are part of the daily routine of companies; they are not going to disappear, the companies must learn how to deal with them. To do so, she highlighted that, first of all, companies must learn to identify the incident, which is often an overwhelming task; next, she emphasized the importance of internal reporting mechanisms, i.e., encourage the use of reports within the company itself to communicate what happened; finally, she highlighted the difficulty and the short period of time to notify those affected by the datat breach, considering the complexity of many cases. On this last point, she emphasized the importance of the Authorities understanding that the first communication about the data breach will be shallower, while the company deals with better understanding what occurred.

Later, **FLAVIA MITRI**, from Uber, spoke. In her presentation, the executive shared a little about the company's experience, which has faced many difficulties in the task of reporting data breaches. She affirmed that, over time, it has built a solid and prepared team to deal with breaches, and the teams work all over the world, complying with the specific rules of the site where the problem was detected. Another point of emphasis concerns the difference in communication about data breaches to the data subjects and to the authorities. For the latter, **FLAVIA** noted that the communication is technical and only occurs when it is legally necessary; as for the data subjects, she stated that the company values a more humanized and careful communication, which occurs regardless of legal imposition.

The fourth expert to speak was **MARIE OLSON,** from Boeing. **MARIE** stressed the importance of adopting an action plan even before the data breach occur, so that the company will have the whole structure ready to execute each of the necessary efforts in the face of the problem. For example, one group will be trying to correct the incident, while another will be investigating the causes, and another will be informing the people needed. Furthermore, small details that are important to avoid data breaches were highlighted, such as encrypting laptop disks, and even giving employees tips on how not to have their machines stolen, such as not leaving them in the front seat of the car or not taking them on trips where they are not needed.

The fifth panelist was **NICOLAS ANDRADE,** from Zoom. He talked about the need to invest in a strong privacy team that develops its work in an integrated way with the rest of the company, an attitude adopted by Zoom, especially because of the great increase in demand

during the pandemic. Moreover, the executive highlighted other important features, such as increasing the time for reporting data breaches to the data subjects and simplifying the breach notification forms, removing, for example, the need for the CPF/CNPJ of the data controller, since there are companies that are not physically located in Brazil.

Finally, **CRISTINE HOEPERS,** from CERT.br, spoke. Cristine made clear the importance of data breaches management, an area within a company that must circulate through data protection, information security, and other sectors. For the panelist, it is extremely important to know what to do before and after data breaches occur, and this is the main role of the data breaches management group. In this sense, she highlighted that one should encourage the DPOs to acquire knowledge beyond the legal aspects of this topic, developing technical skills that are useful for the prevention and control of data breaches.