Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

25 November 2019

Testimony of Bojana Bellamy at the 26 November 2019 public hearing before the Brazil Chamber of Deputies' Special Committee to Issue an Opinion on the Senate's Proposed Constitutional Amendment No. 17-A of 2019

I. Introduction

Good afternoon. My name is Bojana Bellamy. I am the President of the Centre for Information Policy Leadership (also known as "CIPL"), a global privacy policy think tank that is part of the law firm of Hunton Andrews Kurth. CIPL is based in London, Washington, D.C. and Brussels.

Thank you very much for the opportunity to appear before the esteemed members of this Special Committee.

II. General CIPL Background and Work

We work with private sector organizations, regulators and policy- and law makers around the world. Our mission is threefold:

(1) building bridges and driving convergence between national data protection laws globally;

(2) enabling data-driven innovation and the protection of personal data and the privacy of individuals; and

(3) driving constructive dialogue between regulators and regulated organizations.

III. CIPL's Brazil Work

Brazil has been one of our most important focus areas for the past few years during the course of the development of the LGPD and it remains one of our most important areas of interest now that the LGPD has entered its implementation phase until its entry into force in August 2020.

Many of the leading global organizations we work with have significant business operations in Brazil or partner with Brazilian companies. They have supported a national privacy law in Brazil throughout the legislative process that led to the final LGPD. Now our member companies are keenly interested in the effective implementation of Brazil's new privacy law as well as the establishment of a robust and competent national data protection authority in Brazil that can guide them.

Some of you may be familiar with CIPL's active engagement during the LGPD legislative process in the past few years:

- We filed numerous public comments on Brazil's developing privacy law;
- We held numerous workshops and stakeholder meetings in Brazil, often in collaboration with the Instituto Brasiliense de Direito Publico (IDP) in Brasilia;
- We exchanged experiences and views with relevant Brazilian policy and lawmakers on key learnings from around the world, such as in the EU during the implementation of the GDPR, but also in the Asia-Pacific region and the United States.
- And we have launched a new project with our Brazilian partner, the IDP on LGPD implementation. We aim to work with Brazilian companies and the newly appointed DPA to implement the LGPD in a sensible and effective way. This project will, again, be based on a series of conferences, workshops, webinars and white papers.

IV. Discussion

A. The need for centralized and harmonized national privacy protections at the federal level

Let me now turn to the specific questions I have been asked to address today:

- Whether in Brazil data privacy protections for individuals should be provided *exclusively* by one national law, or
- Whether Brazilian States should also be permitted to enact State privacy laws.

I believe that the answer to the first question must be an emphatic Yes and the answer to the second question must be No.

Privacy protections and data protection requirements should be harmonized and consistent across Brazil, and that can only be achieved through one national law applicable everywhere and to all organizations, both in the private and public sector. The LGPD applies nationally to all industry sectors and organizations. As such, it is the proper vehicle for Brazil to ensure strong and consistent privacy protections for all Brazilians regardless of where they are located.

Let me explain my view in greater detail:

About two years ago, Brazil debated the issue of whether the LGPD should also establish a single national data protection authority with oversight and enforcement powers. CIPL strongly supported the establishment of such an authority at the time and submitted public comments to that end with the Brazilian Ministry of Science, Technology, Innovation and Communications (MCTIC) in August 2017. Fortunately, the LGDP now provides for the formation of a national data protection authority, the ANPD.

I believe that all of the arguments that we put forward for the creation of a single national data protection authority are also relevant for having only one national privacy law at the federal level.

Allowing State privacy laws would not only introduce additional and potentially conflicting State privacy protections and rules, but would also bring about a proliferation of competent enforcement bodies and, along with that, the potential for divergent and conflicting interpretations of applicable legal requirements. It would also result in disparate oversight and enforcement approaches across Brazil.

There are clear and compelling benefits to having only ONE national privacy law and only ONE national data protection authority. They include the following:

- Consistency in legal requirements and in the interpretation and enforcement of data protection law, which will ensure legal certainty for both individuals and organizations throughout Brazil.
- Uniform guidance, education efforts and advice on data protection, especially as much of the implementation of the law is left to the data protection authority;
- Consistent enforcement procedures;
- Avoidance of forum shopping by individuals who submit complaints, or by organizations facing sanctions for non-compliance;
- Harmonization of data protection across borders with other nations;
- Having one point of contact with regional and international organizations such as the Global Privacy Assembly (formerly known as the International Conference of Data Protection and Privacy Commissioners (ICDPPC)), the Ibero-American Data Protection Network (RRID), the

OECD, The APEC Cross-border Privacy Enforcement Arrangement (CPEA), the Global Privacy Enforcement Network (GPEN);

- Having one point of contact for international DPAs for cross-border enforcement matters;
- Having one national agenda that takes into account the view of all relevant stakeholders for the development of data privacy law and practices unhindered by the competing and conflicting agendas of multiple authorities.
- Finally, and very importantly, data privacy law is not just about protecting individuals and data. It is also about creating the right conditions for Brazil's digital transformation and for much needed digital trust in the new digital economy and digital society. Brazil needs a Single and Uniform Digital Market, where data can flow and digital services, people and businesses can operate without legal and regulatory fragmentation. This can only be achieved if there is a single federal data privacy law, overseen by a single national data protection authority.

Let me explain some of these points in greater detail.

1. Further explanation of consistency, uniformity and legal certainty

First, consistency in legal requirements and enforcement is important both for individuals and businesses.

Brazilian *consumers* should be able to expect the same level of privacy protections and the same substantive rights regardless of where they are located, who they interact with as consumers and citizens and how they move around Brazil. Fragmented, inconsistent and unpredictable privacy protections will cause individuals to loose trust in the digital economy and undermine their full participation.

Similarly, *businesses* cannot operate effectively in an environment of conflicting and shifting legal standards depending on where they operate inside Brazil. From SMEs to large Brazilian and global companies, they all look for consistency, legal certainty and the ability to improve efficiencies by reducing operational costs. If Brazil cannot provide for this kind of consistency and certainty, it will not be able to fully realize its economic potential in the digital economy, both domestically and globally.

- Companies will not be able to realize operational efficiencies and economies of scale by having the same products or services for all Brazilians.
- Foreign companies may be reluctant to invest in Brazil or will be hampered in achieving effective growth within Brazil if they do invest.
- Just consider the following numbers set forth in a 2017 report by the US Chamber of Commerce on the long term economic impact of a favorable regulatory environment just on Brazil's cross-border information technology and communications services: $1.19 billion added in government revenue; $25.44 billion added contribution to GDP; $5.31 billion in increased investments; and 78,420 new jobs.

This also reflects one of the principal reasons behind the recent EU General Data Protection Regulation (GDPR) – the need to harmonize a fragmented data protection legal regime across the EU and improve its ability to compete within Europe and globally.

Having a single set of rules across the EU was supposed to be a strong incentive for organisations to invest, drive operational efficiencies, and induce businesses to offer uniform services and products across the EU Digital Single Market.

The promise of harmonisation would also bring legal certainty for individuals in the EU, who are increasingly mobile and participating in cross-border transactions.

These same motivations and factors apply in Brazil today and there is a lesson to be learned from the rationale behind the GDPR.

CIPL recently published a paper on the key positive impacts and challenges after 1 year of GDPR implementation. We found that while the GDPR did provide for a single set of rules to a degree, it fell short of its harmonisation aim in ways that have impacted businesses in the EU:

- First, through their own national laws implementing the GDPR, individual Member States have made significant use of the "margin of manoeuvre" provided by the GDPR on some issues. This has led to the creation of differing rules on a variety of issues, for example on age of children's consent, processing of sensitive and biometric data, and scientific research. This resulted in significant administrative burdens and costs for organisations who wanted to implement single compliance solutions.
- Second, national interpretation, guidance and enforcement by EU data protection authorities show that they have diverging views, priorities and approaches (for example they have differing national lists of "high risk processing" requiring a data protection impact assessment). This creates legal uncertainty for businesses.

Brazil now has an opportunity to avoid similar problems by concentrating on implementing one national standard via the LGPD. Fortunately, this may also be easier to do in Brazil than in the EU, which comprises 28 different countries with different languages and legal traditions.

Of course, there are other models for dividing, allocating and sharing privacy oversight and enforcement competency between national and sub-national jurisdictions. Such models can be found in Canada, Germany, Australia and the United States. I don't have the time to address each of them here. I'll simply highlight the example of the United States.

The US currently has a sectoral approach to privacy legislation that provides some privacy protections across much but not all of the private sector. Individual US states are now developing their own comprehensive privacy laws, largely as a reaction to the absence of a comprehensive federal privacy law.

And in counter-reaction to this development towards further fragmentation of privacy requirements across the United States, we are witnessing a broad push to enact a national US privacy law that could pre-empt state laws and would avoid this increasing fragmentation.

Of course, in the US too, the primary motivation is to ensure nation-wide consistency, legal certainty and predictability in privacy protections for the same reasons the EU tried to harmonize its privacy protections and Brazil should pursue a unified national approach to privacy at the federal level.

The way things stand now, I believe Brazil currently has an edge over the United States in terms of ensuring a consistent domestic privacy framework.

2. Further explanation of centralized expertise and international harmonization and coordination

Having only one national privacy law will also ensure that there is one central "expert" authority that can represent Brazil on data protection policy and enforcement issues with one voice, both domestically and internationally.

On the international front, this central authority – the ANPD -- can speak for Brazil on global data protection policy issues and cooperate with foreign counterpart data protection authorities on enforcement matters. The reality of global data flows makes privacy policy and enforcement increasingly a cross-border issue and requires a single data protection authority that can be a steady partner for its international counterparts. Multiple authorities operating under multiple laws cannot do this effectively.

B. Proper resourcing of the ANPD

Finally, let me point out an important implication of having one single law and one single data protection authority: The authority must be properly resourced and with technical knowledge and expertise to implement and enforce that law.

Part of the motivation for having state privacy laws and enforcement authorities may be skepticism about whether privacy can be fully protected with only on cop on the beat – the ANPD.

This is a valid concern and the only way to address it is to make sure that the ANPD is staffed and resourced at a level appropriate for Brazil's size. This includes having sufficient numbers of lawyers, technologists, economists and other professional staff with relevant technical expertise. This is absolutely essential for ANPD in order to be able to discharge its statutory duties provided in the LGPD and to provide the necessary guidance, oversight and enforcement in the complex digital economy.

To give you some perspective of what that would mean for Brazil, the UK Information Commissioner's Office has

- Increased its workforce from 505 to more than 700 employees post GDPR, which represents a 40% increase;
- By 2020-21, it aims to have 825 full-time employees;
- The population of the UK is approximately 66.5 million;
- Brazil's population is about 211 million.

Of course, I'm not suggesting that Brazil should in one fell swoop achieve the same levels of resourcing and staffing.

I am, however, suggesting that a sound national privacy oversight and enforcement framework requires not only a single and consistent privacy standard but also a singular commitment to providing the necessary resources that will give full effect to it.

V. Conclusion

Thank you again very much for the opportunity to share my views and for your attention. I look forward to answering any questions you may have.