

2020 | JUNE



SUMMARY REPORT

DATA PROTECTION REGULATIONS AND THE FIGHT AGAINST COVID-19

WEBINAR OVERVIEW



LAPIN

Dialogues

EUROPEAN UNION · BRAZIL

Report on the “Data Protection Regulations and The Fight against Covid-19” webinar

Executive Summary

On June 12, LAPIN partnered with [EU-Brazil Dialogues](#), a strategic partnership between Brazilian and European institution, to host the webinar **Data Protection Regulations and the Fight against COVID-19**. The event was an insightful opportunity to understand what can be learned from the European experience involving contact tracing tools to fight COVID-19 and to assess the current data protection situation in both Europe and Brazil.

The webinar was divided into two panels, allowing for a global overview of the chosen topics provided by different stakeholders in their presentations. The first panel corresponded to an assessment of the current situation of data protection in Europe and Brazil, for which we counted on explanations provided by representatives from the Brazilian (former) Ministry of Science, Technology, Innovation and Communication - MCTIC¹, [Miriam Wimmer](#), and the Directorate-General for Justice and Consumers of the European Commission, [Bruno Gencarelli](#).

The second panel was dedicated to understanding how data protection is impacted by the use of contact tracing technologies and applications to fight the COVID-19 pandemic. For this segment, we counted on the expertise of actors from multiple institutions; Ms [Laura Schertel](#), professor at the University of Brasília (UnB), and Instituto Brasiliense de Direito Público (IDP); Ms [Carmela Troncoso](#), assistant professor in Computer Science at École Polytechnique Fédérale de Lausanne (EPFL), Mr. [Gwendal Le Grand](#), Deputy Secretary-General at Commission Nationale de l'Informatique et des Libertés (CNIL) and Ms [Verónica Arroyo](#) (Access Now).

A common point observed throughout all presentations was how relevant data has become to our increasingly digital societies, which calls for strengthened attention to **data protection**. While the European Union was able to make use of data responsibly to fight the pandemic, observing its General Data Protection Regulation and reinforcing key elements regarding the data protection matter, few initiatives were able to do so in Brazil, where the entry into force of its General Data Protection Law ended being postponed due to the current circumstances. Below, you'll find a general report covering the most important sharings of the webinar.

Welcome Speech

Ambassador Ignacio Ybañez, Head of the European Union Delegation to Brazil, opened the webinar by stating that since 2016 the European Union has been engaged in the exchange of important views about the data protection matter with Brazil - a process which involves legislative policy, President's office, the ministries of Economy and Foreign Affairs, as well as civil society groups and think tanks. Mr. Ybañez highlighted that the approval of the General Data Protection Law (LGPD), in 2018, represented a pivotal development for data protection in Brazil. Due to the Brazilian LGPD and the two-year anniversary of the European General Data Protection Regulation (GDPR), it seems appropriate for the European Union and Brazil to share ideas and experiences on personal data protection, especially in the context of the COVID-19 pandemic.

Panel 1 - The situation of data protection in Europe and Brazil

1. Miriam Wimmer, Head of the Department of Telecommunications at the (former) Ministry of Science, Technology, Innovation and Communication - MCTIC

Ms Miriam Wimmer's presentation provided an overview about the Brazilian data protection regulatory framework:

- Brazil took an important step in approving its General Data Protection Law (LGPD) in 2018, **allying** with international best practices and with the GDPR. The law was approved after a long-lasting public discussions involving both public and private sectors.
- The issue of personal data protection has always been understood as a part of a strategy to promote the digital transformation of the country, encompassing both the digital transformation of the government and the economy. In this sense, LGPD plays a pivotal role in our legal framework since it deals with the collection, storage, and disclosure of personal data horizontally, being applicable to all sectors of the economy as well as the state. The Regulation, however, has not yet entered into force.
- In parallel, it is important to state that the Data Protection Authority - DPA's creation provisions have been legally enforceable since 2018. Unfortunately, although the provisions of the law, the DPA has not been yet created in fact, since it still necessary a Presidential decree. The absence of a DPA in Brazil is an issue that creates several difficulties, especially during the current period of the spread of the COVID-19. The Brazilian Data Protection Regulation is necessary to issue further regulation to bring clarity to how the LGPD should be applied and interpreted in all the different sectors. On the other hand, although the law is not yet into force, it would be incorrect to state that there is no data protection in Brazil. In fact, several sector-specific laws are covering different aspects of data protection.
- Ms Wimmer also pinpointed out an additional challenge which refers to the COVID-19 pandemic. The sanitary emergency has created a dramatic increase in the need for data processing and data sharing both between the government and private sectors. In parallel, in Brazil, as in Europe, several initiatives have been discussed and adopted regarding the use of technology to combat the spread of the virus such as heat maps and contact tracing apps. But increase data sharing is necessary not only to combat the virus but also to enable the continuity of the regular activities within the government.

In her final remarks, Ms Wimmer expressed hopes that as we face a terrible pandemic, we will also have the opportunity to deep in our discussion and understanding of the importance of data protection legislation and which institutions and policies we need in this field.

2. Bruno Gencarelli, Head of Unit - International Data Flows and Protection at DG Justice of European Commission

Moreover, Mr. Bruno Gencarelli opened his presentation with an overview about the Brazilian and European cooperation regarding the field of data protection.

- In his opinion, data protection is a field where there is a great potential for even deeper mutual beneficial relationship and that can bring benefits to both citizens and business. In Mr. Gencarelli words, “we (Brazil and Europe) need to have similar and robust rules of the game, building a human-centered approach of the regulatory approach in the digital economy, while ensuring that businesses can make the most of digital transformation”. Data protection is a matter of fundamental rights and a democratic imperative according to Mr. Gencarelli.
- In addition, Europe has seen the positive effects of the choice and they published, on June 24th, a [report](#) of the lesson learned in those 2 years of the application of GDPR. Naturally, even though this is a continuous work in progress, positive aspects have been observed regarding multiple stakeholders - citizens, businesses and the government.

In the second part of his speech, Mr. Gencarelli answered the following question: Have the GDPR and other privacy laws passed the test posed by COVID-19? Mr. Gencarelli answered positively to this question and highlighted three main aspects in this scenario:

- “This is actually the first time that we see globally that the necessity of baseline privacy legislation is recognized not as the result of a scandal, as we have seen with Snowden and Cambridge Analytica, but as part of the solution”. This is because data has proven to be a necessary condition to ensure social acceptance of data-driven solutions which were introduced to monitor and contain the spread of the virus, to calibrate public policy countermeasures, to assist patients and help diagnosis, to implement existing strategies, as well as to simply ensure the continuity of government and business operations.
- The crisis has confirmed the validity of the most basics data protection principles. Some key privacy design principles, such as fairness, purpose limitation, transparency and data minimization have proved to be very relevant and pertinent to develop the digital responses previously mentioned. The pandemic also confirmed the importance of having a horizontal framework that covers both the private and public sectors.
- Independent Data Protection Authorities play a key role in data governance. Although sanctions made by DPAs are needed to make the framework functional, one of the most important roles of a DPA is to adapt the interpretation of the rules to contexts that are rapidly evolving. That is why DPAs play a pivotal role in ensuring a consistent interpretation of the law and avoiding those legal uncertainties to be ruled by courts. In the EU, they have seen that DPAs have to step in to assist governments and avoid divergences in interpretation within the members states.

In his closing remarks, Mr. Gencarelli expressed that the European Commission looks forward to closely working with the forthcoming ANPD, the Brazilian Data Protection Authority. As **which will certainly have a important institutional role certainly be a because of all issues mentioned and also for the increasing demand for international standards for corporations. It is very important for them that Brazil could contribute to the development of those standards.**

Panel 2 - Contact tracing and COVID-19: implications for data protection

1. Carmela Troncoso, professor at École Polytechnique Fédérale de Lausanne - EPFL

Ms Carmela Troncoso presented some societal and technical aspects related to the Decentralized Privacy-Preserving Proximity Tracing (DP-3T). Developed by a group of Swiss scientists, DP-3T has been created to be a complement to the traditional manual contact tracing. According to Ms Troncoso:

- The manual contact tracing works like this: once someone contracts the virus, the doctor would indicate that this person should alert others who have contact with them. However, since there are so many infected patients, manual contact tracing has shown its limits. Therefore, proximity contact tracing apps aim to provide a complement by being able to use technology to notify users in a greater scale.
- Some apps are helping to provide a faster and scalable manner to deal with the spread of COVID-19. Moreover, the idea of their approach is to guarantee privacy, by respecting its principles such as data minimization, purpose limitation, and transparency.
- So how their approach works? According to Ms Troncoso, when someone downloads the application, the phone will create a key that is linked to each phone. This key creates random identifiers (random numbers), holding impossible to link directly with that data subject. Moreover, this identifier has a limited amount of time, allowing people not be tracked during locomotion. Then, when those phones are close to each other, they will record each others' random identifiers through Bluetooth. Therefore, after some time, the phone will have hosted two different lists. One is the numbers that have been broadcasted around and the other one is the numbers identified
- For instance, if one of the users unluckily test positive, the doctor will give them a code. With this code, upon consent, users can decide to provide information to a server that helps to notify other users that maybe have been exposed to this positive user. Then, it is uploaded to the server the random numbers produced by the user who has been infected by COVID-19.
- Ms Troncoso alerts that these numbers are not connected to the identity of the owner. They do not reveal the location this person has been. Consequently, these numbers are neither related to the user behavior or other people that this user has seen or interact with.
- Ms Troncoso stated that it is fundamental, from a data protection perspective, whether the system offers privacy-by-design. In this regard, the only information that ever leaves the phone in a DP-3T perspective is the random numbers. They have built the system in a such way that not even the IPs used will be linked to any medical information. Another important feature of the DP-3T is that once the app is excluded, the servers loses any kind of information about the numbers produced by this specific user.

- According to Ms Troncoso, a research agency in Switzerland expects 70% of acceptance by citizens and a lot of this expressive number came from the fact that there has always been transparency regarding the development of the technology. For instance, they have published documents explaining to the public how the application will work, what data will be available and even the protocol of the application.

2. Gwendal Le Grand, Deputy Secretary-General at Commission Nationale de l'Informatique et des Libertés - CNIL

Mr. Gwendal Le Grand opened his remarks stating that since the beginning of the pandemic European Data Protection Authorities have seen an increase in their workload, due to a rise in the number of solicitations regarding data protection, which brought forth the need of a coordinated response. Here are the highlights of his speech:

- The common framework shared by the European Data Protection Board - EDPB and all national DPAs relies on the consistent message that data protection does not impede the fight against the pandemic. GDPR remains applicable, allowing an appropriate response to the pandemic while protecting fundamental rights and freedoms. The increase in DPA's workload shows us that societies are heavily relying on digital technologies and that all digital activities are based on personal data processing operations.
- In this sense, both the EDPB and DPAs have published a series for recommendations, statements, and guidelines to provide guidance and ensure consistency in the various initiatives involving data processing to fight COVID-19. The EDPB, for instance, has released a statement on restrictions on data subject rights in connection to the state of emergency and issued guidelines covering the topics of the processing of data concerning health for scientific research in the context of the COVID-19 outbreak [2] and the use of location data and contact tracing tools in the context of the COVID-19 outbreak [3]. In this turn, CNIL has issued an opinion on the draft decree relating to the mobile application known as "StopCovid" [4].
- The French app's goal is to inform people if they have been potentially exposed to new coronavirus. After being diagnosed with COVID, the app user will receive a QR Code from the medical professional, a code which will then feed the application's system and, therefore, inform its users of potential exposure to the virus.
- There have been discussions regarding how many people should install the app for it to be successful in the fight against the pandemic. Epidemiologists have expressed that even if a small number of people install it, the app will remain useful since it complements the traditional manual contact tracing systems. At the time of the event, there had been already 1.5 million downloads.
- "StopCovid" abides by the French Data Protection Law, collecting and processing data observing the necessity and proportionality principles.

CNIL's opinion states that the app can be useful, but must be considered in the context of a global health strategy. Taking in account that StopCovid is an app that will be formally promoted by governments, the most appropriate legal basis for the data processing consists on the public interest, which, in practice, means that there must be either law or secondary legislation in each Member State to set up the system. Some DPAs warned that choosing consent as a legal basis would bring difficulties to the adoption of the system.

- All data collected via the StopCovid App is being pseudonymized, which means that the application incorporates privacy by design, adopting the most appropriate security measures. For example, the app's system was built in a decentralized manner so that users only have access to the information that they have been potentially exposed, not receiving any specific data regarding another user who has been infected by the virus.

3. Verónica Arroyo, Policy Associate at [Access Now](#)

Ms Verónica Arroyo's presentation covered some of the many initiatives regarding digital technologies and Covid-19 across Latin America. The initiatives mentioned by Ms Arroyo all come from the government and are all different, having its peculiarities:

- In Honduras, a system that covers exposition to the virus has been in place. It is not a contact tracing application, *per se*. In stores and other establishments, people are having their identification documents scanned to understand the circulation of people who have tested positive for COVID-19. If this is the case, the person will receive a notification.
- In the city of Jalisco, Mexico, [a multi-tasker application has been used to fight COVID-19](#). Contact tracing is one of its supported functionalities, using GPS technology in a centralized manner. In the rest of the country, an application called Corona App holds many similarities to the one used in Jalisco. Recently, according to the civil society organization [Karisma](#), it has been found out that the Corona App uses technology provided by [Blue Trace](#).
- In Uruguay, the intentions are to implement the contact tracing functionality to their application by using the API provided by Google and Apple. Differently from other mentioned countries, Uruguay adopts a decentralized approach to contact tracing.
- In its privacy policy, the Peruvian application provides for the erasure of all data after the state of emergency.

When addressing the general situation in Latin America, Ms Arroyo reminded participants that the region still faces a myriad of disparities related to technology.

- Even though technological efforts to fight the pandemic are welcome, issues like digital literacy and Internet connectivity cannot be obliterated. After her overall commentaries on the situation in Latin America, Ms Arroyo

proceeded to talk about the difficulties of finding a healthy balance between the protection of privacy and the promotion of safety.

- As she pointed out, the protection of public security is often used as a long-term goal that justifies privacy violations. Except for Peru, none of the initiatives aforementioned, according to Ms. Arroyo, is clear about what will be done to the collected data. Alongside Uruguay, Peru is also the only country that has expressed in some degree of openness to have its tech solutions audited.

In her closing remarks, Ms. Arroyo stressed her organization's commitment to oversee **if the digital solutions are being deployed to fight the pandemic, due to the necessity of avoiding a legacy of mass surveillance.**

4. Laura Schertel, professor at Universidade de Brasília (UnB) and Instituto Brasiliense de Direito Público (IDP)

Laura Schertel opened her remarks recalling that as the COVID-19 pandemic expanded across the world so did the debates on the use of personal data in the fight against the virus and how that would affect data protection frameworks. Here are the following statements made by Ms Schertel:

- The initial idea of the federal government working with telecommunications companies to verify the population's adherence to quarantine measures was dropped. To this day, there isn't a central contact tracing app being used nationwide in Brazil. Adding to the usual privacy, security, and equity concerns that involve the development of such an application, the fact that Brazil still has insufficient testing would be troublesome to the app's efficacy.
- At the state level, there are several applications used both by governments, universities and research centers dedicated to new coronavirus symptoms. In Ms Schertel's views, the greatest issues in these apps are the purpose and sharing limitations regarding the collect data, which is not well established.
- Another issue refers to the legal basis chosen for these applications: consent. It remains uncertain if the obtained consent was freely given. An app developed by a project related to the University of Brasília, "Guardiões da Saúde - Vigilância Participativa", for example, asks for students and professors to share their health status in exchange for university credits, without clearly establishing the purpose of the collected data.
- The Brazilian Data Protection landscape is currently filled by uncertainty and blurred competences, since the postponement of its General Data Protection Law (LGPD) was approved to August 2021. The Brazilian Supreme Court has ruled unconstitutional a legal provision that mandated the population's data to be shared with its National Institute of Geography and Statistics - IBGE, for statistical purposes during the current state of emergency. If effective, this measure would harvest data (names, cell phone numbers and residential addresses) from more than 140 million

Brazilian citizens. Purpose limitation, transparency, and proportionality regarding data collection were among the objections raised against the legal provision.

- The ruling of the Executive Order n. 954/20 as unconstitutional sets a milestone in the data protection landscape of Brazil overall because of the validation of data protection in the realm of constitutional fundamental rights. Data protection is grounded in different constitutional protections, such as privacy and due process related guarantees, therefore, holding the fundamental rights status.

As Ms Schertel said: "Even though this decision does not neutralize the current general risks to data protection in the country, it does state an important precedent for lower courts" since **adjudication will continue to play an important role in countering legal provisions like the aforementioned executive order while the National Data Protection Authority is yet to be structured.**

Ending Keynote

Mr. Carlos Oliveira, Minister-Counsellor and Head of Digital Market Sector at the EU Delegation to Brazil, proceeded to the meeting's closure by stating that the topic of data protection not only represents an important civilizational value but also a pressing economic matter in the context of the development of the digital economy. The EU Digital Market Sector's representative stated that data protection is very important at the present, among other reasons, because of involving the misappropriation of digital identities, a phenomenon that has increased dramatically. Mr. Oliveira also highlighted interoperability in the data protection field as a matter that has been increasingly discussed. Finally, Mr. Oliveira took the opportunity to thank all participants and express interest in meeting all involved parties in forthcoming events.

Closing considerations

As the COVID-19 pandemic has shown, data protection constitutes a much needed and relevant topic for the development of our societies. As we wait for the concrete structuring of the Brazilian National Data Protection Authority, it is our desire in LAPIN to remain attentive to the multiple developments that are unraveled until then and beyond and the EU Delegation to Brazil is an important partner to be closed to.

End notes

[1] When the webinar occurred, the Ministry of Science, Technology, Innovations and Communications (MCTIC) had just been divided into two different ministries. Now, there are the Ministry of Science, Technology and Innovations (MCTI) and the Ministry of Communications (MC).

[2] EDPB, Statement on restrictions on data subject rights in connection to the state of emergency in Member States, 2 June 2020.

https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/06/edpb_statement_art_23gdpr_20200602_en-1.pdf

[3] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[4] CNIL, Publication of CNIL's opinion on the French "contact tracing" application known as "StopCovid", 3 June 2020.

<https://www.cnil.fr/en/publication-cnils-opinion-french-contact-tracing-application-known-stopcovid>