Despite Provisional Measure, Brazilian Senate passes bill that provides for the coming into force of the General Data Protection Law this year, in August. The Brazilian Internet Steering Committee publishes a statement on the processing of personal data during a pandemic. Microsoft and UnitedHealth launch COVID-19 tracking app for people's return to work. Contact Tracing: how experiences with the technology are going around the world. Stay on top of this and other news in the fifth report of the project "The Data and the Virus".

Senate resumes decision and maintains LGPD starting on August this year

What you need to know...

- Senate vote to make General Data Protection Law in Brazil enforceable by August 2020.
- The rapporteur Simone Tebet said the text was built by experts and so it should come into force at the previously defined date.
- Jair Bolsonaro's Provisional Measure, which postponed the LGPD until May 2021, has not yet been considered by the National Congress and may lapse.

The General Data Protection Law (LGPD in portuguese) had a new chapter in its history on the night of May 19. After having been approved by the Federal Senate to take effect in the country on January 2021, with the application of the sanctions foreseen in the Bill 1.179/2020 on August 2021, the LGPD returns to the original text in terms of its enforceability, which goes back to August this year.

Davi Alcolumbre, President of the Federal Senate, wrote about the decision shortly after the session on his Twitter account: "@SenadoFederal approved, this evening, the anticipation of the validity of the General Data Protection Law (LGPD) for this year, the main legislation in the prevention of criminal attacks promoted by Fake News in the country. The Congress will continue to pay attention to the topic. "

Earlier this month, President Jair Bolsonaro, through Provisional Measure 929/2020, had postponed the validity of the data protection law to May 2021.

The rapporteur in the Senate, Senator Simone Tebet (MDB-MS), defended the maintenance of the original text of Antonio Anastasia (PSD-MG), approved by the Senate in April. She argued that the MP has not yet been considered by the National Congress and that its content may be rejected in its entirety, it may have the provision for the date of entry into force supplied or even expire for not being approved within the constitutional term.

"It is good to remember that this project was formulated by specialists, with the participation of the University of São Paulo and higher courts. The text was created with consensus among the senators", stressed Simone Tebet.

Despite the statement, the text went through another change in the Senate. Senator Weverton (PDT-MA) pointed out that the LGPD will take effect in August this year, with the proviso that the

articles dealing with sanctions will only come into force in August 2021. The senator believes that the change will be important for the treatment of fake news. The highlight was approved, with 62 votes to 15.

"Provisional Measure 959 is going to expire, because it was made to assist in emergency assistance and this is already being done. I have already spoken with several leaders and the Chamber is going to let it expire. So, if the senators wants to help the fake news' fight it is something really important if you think that we are in an election year. We are in the middle of a pandemic, so it should be in force now ", said Senator Wewerton.

Internet Steering Comittee (CGI) writes statement on personal data processing and surveillance during the COVID-19 pandemic

What you need to know...

- Internet Steering Committee in Brazil stated that privacy and protection of personal data are values that must be preserved.
- CGI asked for transparency in data processing, storage and disposal by Apps developed to combat Coronavirus.
- The committee reaffirmed that all technology must be analyzed prior to being put into development and use by the public.

On May 19, the Internet Steering Committee in Brazil (CGI.br) sent a Public Note on surveillance and the use of personal data in the fight against Coronavirus and all the precautions that must be taken by different technologies.

The Committee started the publication based on the use of the powers conferred by Decree No. 4.829/2003, as well as the inc. I, art. 24, of Law 12.965/2014, and also based on the Decalogue Principles of Internet Governance.

The statement was divided into six points, as the first writes about the reaffirmation of the importance of internet and other digital technologies in confronting COVID-19 with the guarantee of fundamental human rights.

CGI also believes that maintaining the population's health, privacy and the protection of individuals' data are values that must be preserved in our society.

CGI warned that the transparency and security of the data must be ensured, as well as the disclosure of treatment procedures, storage, sharing and their disposal. In addition, it provides access to independent audits as a security certifier.

Finally, it reaffirms: “the eventual installation of SARS-COV-2 monitoring Apps must be previously informed to all, in an ostensible manner, observing the principles established by Law 12.965 / 2014,

by Decree 8.771 / 2016 , as well as by Law 13.709 / 2018. Its use should not be used for the stigmatization or discrimination of any segment of the population ".

The entity played a central role in the formulation of the LGPD and in the organization of Privacy Seminars, as you can read in the LGPD Memory project.

Microsoft and UnitedHealth Group launch COVID-19 return to work and symptom tracking app

What you need to know...

- Microsoft and UnitedHealth will use data collection and Artificial Intelligence in a new App.
- Companies will be able to control the security of the workplace through employees informations on the App.
- Microsoft has guaranteed that the data will be UnitedHealth Group responsibility and that it will have no access to any identifiable data.

Microsoft announced the creation of a new App developed in partnership with UnitedHealth Group. ProtectWell ™ aims to act in the process of user's return to the workplace, as well as presenting safe spaces for traffic and companies following all the rules.

The App, according to the company release, incorporates the guidelines of the Disease Control and Prevention Center and studies related to the virus. As in other Apps launched around the world, the user reports symptoms and the technology establishes guidelines to support health and security, as well as the professional's physical space.

The partnership between the two brands combines UnitedHealth Group's clinical and data analysis capabilities with Microsoft's technological leadership. ProtectWell ™ is developed with Microsoft Azure, Artificial Intelligence and analytical solutions, in addition to the existing Healthcare Bot service - collecting data to screen Coronavirus symptoms.

On a day-to-day basis, the App works like this: the user downloads it on the cell phone and answers a group of questions. If the risk of infection is detected, companies can directly send their employees to a simplified testing for COVID-19. In addition, the App gives guidelines and resources to support the security of the workplace area, such as rules of social distance, sanitation and etc.

"While we plan a safe and careful return to workplace, employers need guidelines to ensure a safe office and a robust process for employees to examine their COVID-19 symptoms," said Ken Ehlert, UnitedHealth Group's scientific director.

According to Microsoft, the personal and health data collected by the App will be managed through the acceptance and consent of its users. UnitedHealth will be responsible for the data, and the technology giant will not have access to identifiable information shared by the App.

Microsoft will deploy the service for the return of its employees in the United States.
Private data and Contact Tracing App: what do we know so far about its security?

What do you need to know...

- Chinese government asks citizens to put personal data, including photos, in their Coronavirus tracking Apps.
- UK tests are not conclusive and NHS is questioned about the security and privacy of the data collected.
- Nature release article on Contact Tracing and questions its effectiveness.

In addition to Microsoft, several other companies and governments are investing in Contact Tracing Apps or other technologies in order to monitor cases of Coronavirus, collect data from infected people and try to control the pandemic.

In China, for example, Apps are everywhere and for many different purposes. The authorities collect a great deal of information from their citizens, who do not have the freedom to choose whether to use the Apps or not, since they work on the devices even without consent.

As in other parts of the world, part of the population has not been concerned with the collection of private data by these Apps and governments. “The epidemic is a particular context. Human life is the most important thing, ” told AFP a public official living in Shanghai.

There are several Apps across all the country, some based on geolocation, others on contact tracing and also some that analyze users' health history. What they all have in common is that, after downloading, you need to enter your name, identity number, address, telephone number and sometimes a photo.

“In the end, who has access to this data? Is the data at the mercy of a hacker? We know that the state will not sell the information, but there is always a risk of an employee doing this for their own benefit, ”said Cui Xiaohui, a Metadata and Artificial Intelligence Research Center teacher at the Wuhan University, where the new coronavirus appeared first.

The same concern exists in the UK. On May 18, data privacy lawyers asked the National Health Service (NHS) for transparency on the data storage of the Contact Tracing App that is about to be launched in all the countries where Elizabeth II is Queen.

"Emergencies require quick responses, but those responses must also be appropriate, legal and fair. The current NHS plan to build a large-scale COVID-19 data bank is unlikely to meet these principles. We understand the need for better information on health, but we reiterate that the public must be consulted during the purpose of data storage and be able to obtain adequate information on the

data sharing agreements, "said a group, in a open letter, composed by members of civil society, lawyers and data protection organizations.

The British Intelligence Service's National Cyber Security Center (NCSC) told the BBC, in an interview published on May 19, that it is already aware of most of the issues raised and is in the process of resolving them.

NHS, since the beginning of the Isle of Wight tests, has claimed to treat user data securely and following specifications. Despite this, even the tests in the chosen region are still inconclusive.

On May 19, the scientific journal Nature published an article about the security of Contact Tracing technology and also its effectiveness. Among the issues discussed, the publication highlights the need for humans in order to capture data, information and also care throughout the process of identifying an infected person. As well as the population's need for adherence so that the technology is, in fact, more effective.

“The important thing to understand is that: everything can turns into trash. None of this may work. But, we still have to try. We don't know anything concrete” said Matthew Green, a cryptographer at Johns Hopkins University in Baltimore, Maryland. "We have to try. We just don't know. "

The publication also alerts about the difference between having a centralized technology - when the government itself creates the platform and takes care of users' personal data - and a non centralized system, developed by a company that guarantees their treatment and privacy.

Nature also congratulated the efforts of Apple and Google - a partnership called Gapple - and its concern with data encryption and security protocols.