THE DATA AND THE VIRUS
REPORT #6

Immunity Passport: the best strategy to control COVID-19 or a weapon of discrimination and other problems for society? Brazilian government creates more than 130 public services on digital platforms during the pandemic. GDPR turns 2 and experts question its effectiveness. Contact tracing: how the discussions on technology and application are going around the world. You stay on top of this and other news in the fifth report of the project "The Data and the Virus".

Immunity passport: what experts think and what the risks are for the world population's privacy and data protection

What you need to know...

- Companies create Immunity Passports for countries like the United States and the United Kingdom
- Estonia is testing special document for immunized citizens
- American Civil Liberties Union (ACLU) has expressed concerns about such passports
- Nature magazine listed 10 reasons for not implementing the Immunity Passport around the world

A hot topic for months now in several countries around the world, the so-called ''Immunity Passport'' is still an alternative for some governments, as shown by CNN article in the last week.

Whether via blood tests that determine whether the individual has the necessary antibodies to return to professional activities or through documents and applications, the topic has gained discussion in major media outlets, in addition to NGOs and research groups.

According to a Forbes publication, a startup named FaceFirst, located in California, United States, is promoting the idea of a ''record of immunity to Coronavirus''. The technology is based on a database fed by the health system which reports on the immunity status of citizens. To access data about tests performed, viral load received and other possible information about contact with the virus, the user must unlock the system with facial recognition.

The company's CEO, Peter Trepp, believes that the measure can bring many benefits in different places and times. "I believe that, collectively, data can be useful in determining how you fill an airplane, for example. You can fill a flight with people free of the virus and another with passengers who are already immune ", he explained.

Trepp also believes that the "Immunity Passport" will be important for the moment the vaccine is discovered, so that priority is given to those who have not had contact with COVID-19.

In the UK, the company Onfio has proposed a similar project, a system for citizens, guests and employees to have proof of immunity so they can prove their health status. In this case, they must perform facial recognition, but without the need to share other personal information.

''Technology is used to link a human being to his digital identity, using only a photo and a video in selfie format. The results of the exams will be linked to the image and the digital certificate can be displayed, such as boarding passes for smartphones, "said Husayn Kassai, CEO of Onfio.

While countries are still discussing the feasibility and feasibility of the document, Estonia has already started testing its digital passport, according to a [report](#) by the Reuters news agency.

Taavet Hinrikus, founder of Transferwise and a member of Back to Work, a non-governmental organization that develops the passport, told the publication that the document aims to alleviate fears and encourage societies around the world to move on with their lives in the midst of the pandemic.

Despite the efforts by technology companies and governments to show the positive side of the passport, the anxiety over the possibility of monitoring of medical records is clear.

Last week, the American Union for Civil Liberties (ACLU) [expressed](#) concerns about such passports, saying that the new health surveillance infrastructure certainly jeopardizes privacy rights.

The Organization also noted that such a measure will divide the population between immune and non-immune. "Unimmunized people are unlikely to have an advantage when competing for a job with someone with antibodies, for example," he warned.

Who was also opposed to the creation of the Immunity Passport was the [World Health Organization](#). Among its main reasons is the fact that it has not yet been scientifically proven that those infected with COVID-19 are in fact immune to the disease.

Nature Magazine also talked about the subject in an [article](#) and listed ten reasons why creating a document such as this would be impractical, unfair and unsafe for the general population. In addition to the unknown behavior of the Coronavirus in the human body is the unreliability of the existing tests, since most tests that detect antibodies have high rates of false positives and negatives.

The lack of tests for citizens was also an important factor, since most people have not been tested. The publication said that if only the immune people were to be released in order to resume the economy, for example, the number would not be enough to make the plan effective.

''Low disease prevalence combined with limited testing capacity, not to mention highly unreliable tests, means that only a small fraction of any population would be certified as free to work'', they remarked.

Nature still points to monitoring as a factor that compromises privacy, which can cause the marginalization of the non-infected or even greater racial or social segregation. Such factors can lead to intentional infections by people who do not wish to be labeled as vulnerable and suffer possible discrimination.

''The immunity passports of today could become the all-encompassing biological passports of tomorrow'', they concluded.

Government creates more than 130 public services on digital platforms and personal data may be at risk

O que você precisa saber…

- Since the beginning of the Coronavirus pandemic, more than 130 public services have been launched on digital platforms
- According to InternetLab, the apps do not provide users with guarantees of privacy and data protection
- Organization Idec publishes list with best practices in the use of personal data

Home office, videoconference meetings, calls and a whole digital transformation that would eventually happen in years, but ended up taking place in months. This has been the reality of the whole world in recent months and, of course, in Brazil.

During the pandemic period of the new coronavirus alone, the federal government announced the creation of 130 digital services, according to an article by Agência Brasil. The online applications and services created facilities for a part of the population, but also brought exclusion to the unconnected part and jeopardized the protection of personal data.

Among the most sought after services are emergency assistance, unemployment insurance requests, salary allowance, issuing of proof of the Single Registry and obtaining a work card.

Launched to prevent contagion and bring information about the disease, the coronavirus-SUS application has already reached 14 million unique accesses, according to a special website made by the Ministry of Health.

The Reseach Center on Internet and Society InternetLab analyzed several applications, including from the Federal Government, investigating aspects of privacy and data protection.

The organization identified high risk exposure, including in coronavirus-SUS and emergency assistance applications, in relation to guarantees defined in the legislation.

"If the analyzed applications do not inform about the treatment they carry out for the purposes of the app, they also do not do so regarding any eventual further processing of the data, that is, for other purposes besides those that the user has consented to. Considering the potential that the collected data has to provide information and to qualify the public debate and research regarding the pandemic, these new uses should be considered", informed the study's authors.

And it's not just public apps that cause a lot of concern about privacy and security of personal data.

The Brazilian Institute for Consumer Protection (Idec) also expressed its opinion regarding the risks of exposing the personal data of millions of users, both in government applications and in several others, such as e-commerces and etc.

The pandemic has intensified the use of personal data and the digital tracks collected by cell phones. In addition to the registration of users on the platforms, one of the most relevant data in this period is that of geolocation, widely used as a possible containment tool for COVID-19.

The publication highlighted the delay in both the coming into force of the General Data Protection Law in the country and the creation of the National Data Protection Authority (ANPD). "It is important to note that principles related to the right to privacy and data protection are present in national laws well before the LGPD, such as the Consumer Protection Code, the Access to Information Law, the Civil Rights Framework for the Internet and the General Law of Telecommunications, as well as the Federal Constitution", he added.

The organization listed, in an article, five basic recommendations for the safe sharing of location data, together with guidelines to avoid violations of rights. Among them are transparency in the use of data, anonymization, safe disposal and non-discrimination. Check out the full list.

The coordinator of the Data Privacy Brasil Research Association Rafael Zanatta spoke about the risk of misuse of personal data and also about the importance of the General Data Protection Law in guaranteeing the privacy of the population in the country. Check out the interview for TV Senado.

Also check out the Rafael Zanatta's interview on the risks of surveillance in the pandemic.

In the midst of the pandemic, GDPR completes two years of challenges, under question and with a long way to go

What you need to know...

- On May 25, the General Data Protection Regulation (GDPR) completed two years.
- NGO Privacy International published a report on the law, its victories and its failures.
- European Digital Rights (EDRi) has published an open letter to law regulators.
- None of Your Business (NOYB) made several considerations about GDPR, focusing on "how" to create technology in accordance with the law to fight COVID-19.

May 25 was marked by the [2nd anniversary](#) of the General Data Protection Regulation (GDPR). Two years ago, the law was intended to punish invasive practices and misuse of personal data by large companies and the public sector. Throughout this period, the law has shown itself to be present, even though, at times, it suffers from a lack of supervision, insufficient funding and limited resources.

The law became even more prominent with the arrival of the new Coronavirus pandemic and, consequently, the creation of applications and technologies that aim to contain the virus, using an extensive personal database for this purpose.

The NGO Privacy International has taken [stock](#) of GDPR since its creation, going through victories achieved and also the long road that the law still has to go. The publication cited several companies, such as Facebook, elections and even the Cambridge Analytica case.

The organization showed concern about the lack of inspection and the lack of accountability of the companies. "These infractions not only further exacerbate the opacity surrounding the online data ecosystem, but also constitute a major obstacle to the effective exercise of data subjects' rights, effectively undermining the protection offered by GDPR and people's confidence in the law to protect fundamental rights" he added.

Regarding the application of the law on technologies created to combat COVID-19, Privacy International has shown disappointment, stating that, unfortunately, attention to transparency and purpose limitation has not had an effect in the United Kingdom and countries that make up the European Union.

"GDPR is a long-term project. The past two years have barely given us an idea of whether this project will be successful, "said Eduardo Ustaran, who heads the privacy practice at London law firm Hogan Lovells International, in an [article](#) published by Estadão.

European Digital Rights (EDRi), to celebrate the commemorative date, wrote an [open letter](#)to GDPR. In it, it shows a series of flaws, as well as a lack of resources, and even points out inefficiency of law enforcement in cases of abuse of consent, failure to access behavioral profiles and lack of transparency of companies.

While some publications show doubts about the law's effectiveness during this period and also its role during the pandemic, The New York Times published an [article](#) stating that GDPR is a great

"watchdog" for the population, keeping it safe - or in the way of - personal data and corporate transparency.

None of Your Business (NOYB), [published a study](#) on GDPR in the midst of the new Coronavirus pandemic and also made a special article, talking about the lack of understanding between the possibility of law enforcement in technologies to combat COVID-19 and the illegality of the presentation of some applications, signaling that the correct question to be debated is not "if" but "how" to do this in the right way.

Max Schrems, honorary president of noyb, [said](#): "GDPR explicitly provides for data processing in the fight against epidemics. Data protection laws should therefore not be 'waived', but simply observed ".

Contact Tracing: what NGOs and Data Protection experts think

What you need to know...

> - Countries around the world are looking for technology to control the new Coronavirus.
> - NGOs believe that digital work should be linked to government public health plans.
> - Despite the strong role during the pandemic, Apple and Google are still the target of doubts and criticism.
> - Data transparency is the most worrying point in using Contact Tracing, in addition to its real effectiveness.

The world is in the technological race to discover the best way to fight the new Coronavirus. As companies around the world rush to find the right and most efficient way, the population becomes increasingly afraid and specialists are more concerned with the consequences of products that disrespect privacy and the unrestrained use of personal data.

On the subject, the NGO Privacy International wrote an [extensive article](#) on the "mess" that Contact Tracing has become around the world. The publication talks about the urgency of governments to find a quick formula to fight COVID-19, without relying on science to create vaccines, drugs or the need to create hospitals and other high expenses.

"It is not clear whether some of the data generated by cell phones is useful; and they will not be as reliable as manual contact tracing. Making applications mandatory will increase inequality. No government has ever known you as much as it may be about to" , said the organization.

Despite this, members of the Swiss army, hospital workers and public officials can install the SwissCovid app prior to a wider planned deployment in the country, according to a [BBC report](#).

The technology chosen by Switzerland was developed by the Apple-Google partnership and involves tracking contacts to detect when two people are close and if there is a risk of contagion between them.

Like Switzerland, Latvia has also started testing the platform of the world giants. The technology is known as decentralized, meaning it does not provide personal data to governments on a centralized basis. However, it still causes discomfort on the part of specialists.

In a recent publication, Privacy International questioned whether the reputation of Apple and Google during the days of COVID-19 would be sufficient to erase their entire past. The publication also cited a recent fact, in which a former Apple employee said it was possible to listen to recordings of the brand's users through Siri.

The organization added: "Our personal data, including data about our health, is at the heart of these companies' business model, as they are an essential input to the training of AI models, including search engine results. Our data is the product they market. And given the growing importance of data in all sectors of the economy, this concentration is expanding to other sectors, such as health. "

In this scenario, countries such as the United Kingdom, France and some regions of the United States have chosen to create their own applications in order to retain all user information. However, most of them have already had some kind of flaw, either in the privacy policy or through the leakage of personal data.

According to The Independent, Care19, created for South and North Dakota, has been selling data to outside companies, despite not showing it in its privacy policy.

This brings even more insecurity to its users. According to Check Marx, more than half of the American population is not willing to join Contact Tracing as a means of fighting the pandemic.

The NGO Algorithm Watch published a series of observations on the subject, making considerations about the use of applications as "saviors" of COVID-19 and alerting to other necessary fronts.

''The COVID-19 is not a technological problem. Analyses of actual responses to the outbreak show that successful interventions are always grounded in broader public health policies. Singapore, South Korea and Taiwan, frequently cited as role models in keeping the epidemic in check, all had plans in place, most of them designed after the 2003 SARS outbreak. Preparedness for an epidemic reaches beyond technical solutions: it means having resources, competences, plans, and the political legitimacy and the will to quickly deploy them when needed.''

DOCUMENT LICENSE

TEAM

Project "The data and the virus". Data Privacy Brasil Research Association. Coordination: Rafael Zanatta & Bruno Bioni. Research team: Mariana Rielli, Gabriela Vergili, Iasmine Favaro and Carolina Pain. Support: AccessNow.

PRESS

For contact with press relations and requests for collaboration (interviews and podcasts), please send an email to press@dataprivacybr.org. Information about the project can be found at dataprivacybr.org