ISSN 1982-0496



# *SENSITIVE PERSONAL DATA ON HEALTH AND LIMITS TO THE FLEXIBILIZATION OF THE RIGHT TO PRIVACY IN THE CONTEXT OF COVID-19 IN BRAZIL*

## *DADOS PESSOAIS SENSÍVEIS DA SAÚDE E LIMITES À FLEXIBILIZAÇÃO DO DIREITO À PRIVACIDADE NO CONTEXTO DA COVID-19 NO BRASIL*

---

**Gianfranco Faggin Mastro Andréa**

Doutorando e Mestre (2017) em Direito Político Econômico pela Universidade Presbiteriana Mackenzie. Especialista em Direito Público pela Faculdade de Direito Damásio de Jesus (2007). Professor de Direito na Universidade Santa Rita. Professor de Direito da Universidade Paulista. Analista do Ministério Público da União.

**Wagner Wilson Deiró Gundim**

Pós Doutorado pela Mediterranea International Centre for Human Rights Research, em parceria com a Università Mediterranea di Reggio Calabria (2020-2021), com bolsa integral. Doutor em Filosofia do Direito pela Pontifícia Universidade Católica de São Paulo – PUC/SP (2020), tendo sido bolsista CAPES. Doutorando em Direito Constitucional pela Faculdade de Direito da Universidade de São Paulo – FADUSP (2021). Mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie (2017). É Líder do grupo de pesquisa "A circulação de fluxos informacionais e a lei geral da proteção de dados brasileira: perspectivas e desafios", vinculado à Universidade Anhembi Morumbi. É Vice-Líder do Grupo de Pesquisa Cidadania, Constituição e Estado Democrático de Direito, vinculado ao Programa de Pós-Graduação Stricto Sensu da Universidade Presbiteriana Mackenzie, bem como integrante dos seguintes grupos de Pesquisa: 1) Os Parlamentos Latino-Americanos, vinculado ao PPGD USP; e 2) Grupo de Estudos em Direito, Análise, Informação e Sistemas (PPGD PUC/SP); e 3) Hermenêutica e Justiça Constitucional: STF, vinculado ao PPGD PUC/SP. Professor da Faculdade de Direito da Universidade Anhembi Morumbi.

**Abstract**

The COVID-19 pandemic exposed the deep blemishes of inequality surrounding the world, but also unveiled the multiple possibilities for



DOI: 10.25192/issn.1982-0496.rdfd.v26i22145

applying new technologies to confront and control the spread of the disease. Big Data technology linked to geographic and contact tracing emerges as a real possibility for disease control. However, the rising problem consists of the excessive flexibility of the right to privacy and to the protection of sensitive personal data, which deserves the creation of beacons to impose limits on the collection and processing of data without purpose deviations. The article aims to shed light on the necessary balance between the right to privacy and the right to health, with focus on the protection that should be guaranteed to sensitive personal data. For this purpose, bibliographic review methodologies were used, as well as-state-of-the-art topics such as surveillance and the right to privacy. Finally, it was concluded that there is a possibility to establish limits to the flexibilization of the right to privacy and data protection in Brazil even when facing emergency situations, guided by principles such as necessity, purpose, reasonableness and proportionality. Brazil shows delay in the incorporation of such new technologies, which is suggested for future confrontations of new pandemics.
**Keywords:** COVID-19. Health. Right to privacy. Sensitive data protection.

**Resumo**

A pandemia da COVID-19 expôs as profundas mazelas da desigualdade ao redor do mundo, mas também desnudou as inúmeras possibilidades de aplicação de novas tecnologias para o enfrentamento e controle da disseminação da doença. A tecnologia do *Big Data* atrelada ao monitoramento geográfico e o *contact tracing* exsurgem como reais possibilidades de controle da doença. Contudo, o problema que surge consiste na demasiada flexibilização do direito à privacidade e à proteção de dados pessoais sensíveis, que merece o estabelecimento de balizas que imponham limites a coleta e tratamento de dados sem desvios de finalidade. O artigo objetiva lançar luzes sobre a necessária ponderação entre o direito à privacidade e direito à saúde, com enfoque na proteção a ser garantida aos dados pessoais sensíveis. Para tanto foram utilizadas as metodologias de revisão bibliográfica, bem como do estado da arte de temáticas como vigilância e direito à privacidade. Por fim, concluiu-se que há a possibilidade de estabelecer limites à flexibilização do direito à privacidade e proteção de dados no Brasil mesmo diante de situações emergenciais, pautando-se por princípios como da necessidade, finalidade, razoabilidade e proporcionalidade. O Brasil demonstra um atraso na incorporação dessas novas tecnologias, o que se sugere para enfrentamentos futuros de novas pandemias.
**Palavras-chave:** COVID-19. Direito à privacidade. Proteção de dados pessoais sensíveis.

## 1. INITIAL CONSIDERATIONS

The first quarter of the 21st century, while demonstrated the enormous

capacity of human civilization in terms of disruptive technological advances to improve and facilitate life, also exposed the fragility of human life in face of the world pandemic of the new coronavirus.

The fourth industrial revolution (SCHWAB, 2016), guided by technology and accompanied by the globalization that was already occurring, made the term "distance" something totally relative. However, if on the one hand technology and globalization made the world more accessible to most of the population, the rapid circulation of people around the globe was demonstrated as an issue when it comes to the spread of infectious diseases.

By the end of December 2019, the first known case of a new virus emerged, one that rapidly spread across the globe. About two months after the first case, the World Health Organization (WHO) declared the state of world pandemic, faced with the velocity and high contagion rates worldwide.

Humanity has already faced several outbreaks of infectious diseases since the beginning of the 21st century, but the new virus – despite its low lethality rate, of around five percent – presented a high rate of contagion, capable of collapsing countries' entire health systems, if containment measures were not adopted.

Issues of inequality between countries in the global south and global north (SANTOS, ARAÚJO, BAUMGARTEN, 2016)[1] regarding basic sanitation, healthcare system, education and housing were completely exposed as the new virus advanced. The pandemic brought several lessons which deserve further reflection in the future, but one issue that became evident concerns the collection and treatment of personal heath data of the population by the use of new technologies, in order to combat the spread of the new virus.

Therefore, what would be the limit for the relativization of the right to privacy facing the pandemic of the new virus in the health field, knowing that the access to sensitive personal data of the population may assist in the prevention and real-time monitoring of the spread of infectious diseases? That is the problem the present article aims to answer.

For such, the methodology used was the bibliographical review of academic

[1] It is important to highlight that the concepts of north and south do not reffer to geographical localizations, but to a distinction formulated by Boaventura de Sousa Santos, to whom the global north represents the developed countries and the global south is a "metaphor of human suffering caused by capitalism, colonialism and patriarchy, and of the resistence to such forms of opression" (SANTOS, ARAÚJO, BAUMGARTEN, 2016).

and scientific production related to the new coronavirus between December 2019 and June 2020, an opportunity in which the following words were searched together in Google Scholar: “COVID-19”, “BIG DATA”; “LAW”, and “PRIVACY”. 1.820 (one thousand, eight hundred and twenty) articles were found as results, of which 20 (twenty) were selected to be used in the present study, after analysis and filtering. Furthermore, the state-of-the-art methodology regarding themes such as right to privacy and surveillance was used as context to the development of arguments and comprehension of the tensions between the fundamental right to sensitive data protection and the supremacy of public interest over the particular one, when it comes to controlling the spread of the disease.

The first part of the article involves a chronological presentation of the new virus pandemic around the world. Secondly, we seek to understand the big data technology as applied in connection to personal data and its potential in combating the new virus. In the third section of the article, the question involving the tension between the right to privacy and the right to health in terms of data collection is deepened. Finally, the concept of sensitive personal health data and the limits of its use in the context of combating the new coronavirus in Brazil are analyzed.

## 2. COVID-19: THE PANDEMIC THAT TRANSFORMED THE WORLD OF THE BEGINNING OF THE 21st CENTURY

The coronavirus (known as COVID-19[2]) emerged in the town of Wuhan – China in December 2019[3] but was only recognized by the Chinese authorities as a new virus in January 2020. It is a highly infectious disease that causes serious acute respiratory syndrome (BOULOS, GERAGHTY, 2020, p.1). The World Health Organization (WHO) declared the new coronavirus as an international public health emergency issue only in late January 2020, as the disease was spreading rapidly around the world (SHAW, KIM, HUA, 2020, p.1). As the present article is being written, COVID-19 has already infected over ten million people in the world and caused the death of around 520.000,00 (five hundred and twenty thousand) people.

[2] “COVID” means Coronavirus Disease, as “10” refers to 2019, when the first cases arising in Wuhan, China were publicly exposed by the Chinese government, by late December. The denomination is important in order to avoid cases of xenophobia and prejudice, as well as possible confusions with other diseases (FIOCRUZ, 2020).

[3] It is important to highlight that the dawn of the new coronavirus is still uncertain. However, the epidemic took shape primarily in the Chinese city.

Over six million people have recovered from the disease[4].

Chinese authorities sought to contain the virus. However, due to its rapid contagion rate, it ultimately reached multiple other areas in China and, subsequently, the world. The first reported case out of China occurred in Thailand in January 13th, 2020.

In early February 2020, Italy, in turn, declared a national emergency with two reported cases. As the virus continued to spread across China and other countries, WHO named it "COVD-19", unifying the form of reference to the new disease. A few authorities were appointed by WHO as of February 21st, 2020, in order to advice different countries. Several missions were organized by the WHO team: in Italy (February 24th, 2020) China (February 25th, 2020), and Iran (March 2nd, 2020) (SHAW, KIM, HUA, 2020, p.2).

As of February 24th, the pandemic epicenter shifted from Chine to other countries. Besides Japan, the two other great epicenters were Iran and Italy. Between the 6th and 7th of March 2020, the virus had already affected over 100 (one hundred) countries and 100.000 (one hundred thousand) people. In light of such scenario, WHO declared, in March 11th 2020, that the advance of the disease was to be considered a global pandemic, given circumstances such as: rapid dissemination worldwide; higher lethality rate among the elderly and carriers of pre-existing comorbidities (e.g., diabetes and other chronical illnesses); and different recovery rates (SHAW, KIM, HUA, 2020, p.2).

United States of America declared national emergency in the 13th of March 2020. Thus, after China, the epicenters of the disease moved around the world, an opportunity in which, until the time of writing this article, epicenters were found first in Italy and Spain, then England and the United States, and now Brazil.

The disease's devastating consequences are unprecedented to globalization. The greater access of people to travel by air and the concept of making the world increasingly connected and globalized ended up accelerating the spread of the disease in different parts of the world. Despite good prospects, there is still no vaccine for COVID-19; it has been estimated that its production may take about a year, which imposed on governments the adoption of social distancing measures.

[4] To access fully updated numbers, r. Worldometers.info (2020), https://www.worldometers.info/coronavirus/.

The social distancing[5] measures adopted around the world consisted of what was conventionally called “social isolation”. That means all citizens, to the extent of their possibilities, must remain in their homes, which should be left only in order to provide for essential activities, such as shopping for food and medicines. Such a way of coping with the disease sought to reduce the contagion curve, so as to not collapse the healthcare systems. In a certain percentage of cases, the disease can generate the need for hospitalization in Intensive Care Units (ICUs), which have a limited number of beds. That is, if the disease were to spread without control, the number of beds would prove insufficient to the amount of seriously infected patients.

Many countries resisted the imposition of social distancing due to the negative impacts it would have on the economy. The government of Italy, for example, delayed adopting the measures recommended by the WHO, which ultimately caused a collapse of the health system and lead to the death of thousands of people.

Thus, in the absence of a vaccine, what remained was the adoption of measures to reduce the spread of the virus, precisely by reducing personal contact through social isolation. Some protocols have also been adopted in several countries (OLIVER et al., 2020, p.1).

The pandemic, however, highlighted something that already existed, but which remained latent: the extreme socioeconomic inequalities. Those most affected by the pandemic are surely the poorest populations in underdeveloped and developing countries. When taking into consideration countries where the access to full basic sanitation, drinking water and electricity has not been achieved, countries in which people live in a state of extreme vulnerability (e.g., slums), it is highly utopian to predict that social distancing measures could be met (SANTOS, 2020). In such peripheral locations, whole families share shacks of only a few square meters.

However, what is worth mentioning is the use of technology as an ally in the fight against COVID-19, precisely to identify areas of risk and serve as a parameter for government decision-making. Technology is inextricably linked to the development of countries. In the current period, it is necessary to highlight that the implementation of public policies that meet the development goals must be guided and make use of technological innovations as instruments of social emancipation,

[5] To access further information on the effects of social distancing and its psychological effects, see A.S.M Kayes et al., *Automated Measurement of Attitudes Towards Social Distancing Using Social Media: A COVID-19 Case Study*, PREPRINTS (2020).

whether in the areas of health, education, housing, basic sanitation, etc (BENKLER, 2005, p. 12).

Having established the premise of technology as an instrument to combat inequalities and a means to achieve goals, it is important to highlight its role in the context of the pandemic and the consequent tensions arising from its use, notably regarding the collection and manipulation of sensitive personal data. This is what this article seeks to analyze below.

## 3. BIG DATA TECHNOLOGY IN THE FIGHT AGAINST COVID-19

Several countries have certainly used technological innovations as weapons to combat the spread of COVID-19. The revolution through the so-called Big Data spreads over several areas and, certainly, the field of research on infectious diseases is not immune to such technological innovations. Big Data means advanced analytical method of processing, regardless of the size, type, or format of data (BANSAL et al., 2016, p.375).

It comes to the possibility of data mining at high speed and performance, in order to obtain information[6]. The three terms "V": volume, velocity, and variety, are often associated with Big Data, in reference to the amount of data, the increase in speed regarding collection and use and the different types and ways of obtaining them. Other qualifiers are also added to Big Data, such as veracity, validity, volatility, and value, insofar as it always seeks to meet the need for precision, permanence power and usefulness of such data (BANSAL et al., 2016, p. 375).

The use of Big Date to combat infectious diseases involves three types of data flows: medical data, patient information data, and digital data not directly related to health. Medical data flows can be obtained from the records of hospitals, health insurers and death certificate records. In this case, the reported data are able to

[6] One must here highlight that the analysis of data through Big Data technology is performed based on an inductive data logic, as highlighted by Márcio Pugliesi and André Martins Brandão: “The analysis of a large amount of data through big data technologies is mainly focused on finding correlations - recognizing patterns, which refers to inductive logic. Traditional Cartesian scientific thinking works mainly with deductive logic. Traditional forms of data analysis also work with a kind of deductive data logic. It is at this point that big data diverges from both traditional forms of data analysis and classical scientific thinking, as it works from an inductive logic of data. [...] Big Data technologies are guided by a kind of inductive logic, with the purpose of guiding the subject in the complexity of the data ocean, enabling the instant search for crucial information - singularities in complexity, correlations or patterns, the processing of them as a whole without preconditions, the effective reproduction of mechanisms observed in the past and the generation of information that can be used in the present, guiding actions aimed at the future ” (PUGLIESI; BRANDÃO, 2016, p. 461).

guarantee the observance of the disease status, which can be monitored individually or in an aggregated way in the geographical scope (BANSAL et al., 2016, p. 376).

The data in the second category are those obtained as a result of information about voluntarily self-reported symptoms. In this case, there is no confirmation of infection for a specific pathogen, but it can assist in the production of health data on an individual level and practically in real time.

In contrast to previous flows, one can use Big Data related to data not necessarily linked to health, that is, that do not depend on specific patients, but derive from internet search tools, social networks, and cellphones. These data flows inform about health-related behavior, including contact and travel patterns, vaccine status and feelings, which are key ingredients for understanding and transmitting disease (BANSAL et al, 2016, p. 376).

Some experiences using Big Data in the monitoring of infectious diseases such as H1N1 demonstrated the potential of its use, as it can improve control of both dissemination and resolution, in addition to providing access in relation to “hidden” populations, unobservable without the Big Data system. However, the promise of these new technologies must be adopted with caution. On the one hand, the ample access to data (necessarily medical, obtained by companies in the private sector) and its rapid processing lighten unprecedented details as to the way pandemics spread; on the other hand, they point to its underutilization due to fear of privacy issues and barriers to access to e-health (electronic health data) by the academy and governments. It is also noteworthy that some instruments such as Google Flu Trends (GOOGLE, 2020)[7] may incur in errors as a result of excessive measurement or of an abrupt extinction of the disease. This issue is particularly salient after profound disturbances to the dynamics of the disease, as is the case with the emergence of a new pandemic virus (BANSAL et al., 2016, p. 376).

Therefore, perhaps the best way to understand and monitor infectious diseases is to use Big Data, but in a hybrid way, that is, an integration of digital Big Data with traditional laboratory bases for observation and control, as well as e-health data to improve the punctuality, accuracy and depth of existing surveillance indicators. To count on the voluntary participation of the population informing any symptoms of diseases or adverse effects of medications, albeit through social

[7] For more: https://www.google.org/flutrends/about/.

networks, also presents itself as a database of great potential (BANSAL et al., 2016, p. 376). The problem here is the accuracy of what is collected on social networks and possible false alerts.

The application of Big Data in the monitoring and forecasting of pandemics certainly still requires some maturation and development in order to avoid possible mistakes, either due to methodological challenges (uncertainties in dissemination), or due to the effectiveness and impact of new associated technologies without academic validation or scientific. One can even point to the challenge regarding misaligned investment depending on each country, capable of preparing health professionals regarding reporting epidemiological data accurately during an epidemic (BUCKEE, 2020). In any case, the increment of a hybrid system may be able to generate greater precision, as the technology of surveillance and monitoring guided by Big Data advances.

Regarding the application of Big Data by China - the first country to notice the emergence of the virus - in the fight against COVID-19, the Government used Baidu Big Data to identify groups of infected people. People's mobility data were used to monitor movements from one location to another during the beginning of the disease spread stage, which ultimately assisted in making decisions about the lockdown decree in areas at a higher risk of contamination. It was also used in the process of reopening shops and factories to identify potential risk areas (SHAW, KIM, HUA, 2020, p.8).

With regard specially to the application of big data to deal with Covid-19, as Bethania de Araujo Almeida et al well affirms:

> Considering the difficulty of diagnosing the infection in the general population, technological initiatives have been developed to make it possible to track symptoms, contacts and displacements considered important components to support strategies for monitoring and surveillance of contagions by governments. Big bets have been placed on the development of applications that collect personal data, geolocation, and movement of people. Such practices raise questions about the types and amount of data needed, and the ethical, legal, and technical challenges that permeate the collection, access, sharing and use of this data. Apple and Google recently entered a partnership to ensure interoperability between iOS and Android systems to create a tracking tool for COVID-19. According to the companies, people will have the option to participate, but they do not mention the option of withdrawing consent at any time. The system, according to published specifications, has similarities with solutions that have been referred to as 'contact tracing' and are broadly inspired by an already operational implementation in Singapore and proposals under development in Europe such as DP-3T (Decentralized Privacy -Preserving Proximity Tracing) or the

> PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) project. This proposal, like MIT's Safe Paths Platform, seeks to maximize privacy. In general terms, these solutions, which fall into the classification of Contact Tracing systems, work with the exchange of anonymous identifiers between nearby phones via Bluetooth, after installing an application made available by the national health authority or eventually by the operating system itself, depending on how the solution operates. When a person has a positive result for the coronavirus, he or she will register it in the application, which will transmit the data to health authorities in the respective country. Then, people with whom one has had contact in the previous 14 days will be alerted that they have been in contact with someone who has been diagnosed with disease. As these are technologies that are still in the development and maturation phase, there are differences between implementations that, over time, can prove to be very significant, as, for example, it already seems to be the centralized focus of the PEPP-PT in contrast to the decentralized DP-3T. The panorama points out that, in the next phases in which society will be adapting to live with the virus, the use of personal data and applications or devices will play a prominent role not only in measuring contact, but for purposes such as verifying compliance isolation, quarantine, probabilistic contagion verification, managing permissions for people to go out in public, among many others (ALMEIDA et al., 2020).

As it is clear, although the use of technological devices and data collection classified as sensitive is shown to be necessary to deal with the pandemic crisis experienced by the world, the perspective is that the degree of use and manipulation of this data by new and varied tools ultimately focuses on the space of citizens' right to privacy and intimacy, which can lead to a critical situation of tension between extremely relevant fundamental rights. Hence the need to analyze the possible collision between the right to privacy and the right to health, in exceptional situations such as the present.

## 4. THE USE OF BIG DATA BY GOVERNMENTS: THE TENSION BETWEEN THE RIGHT TO PRIVACY AND THE RIGHT TO HEALTH

In the health field, it is possible to state that the application of Big Data technology is here to stay (ABOUELMEHDI, BENI-HESSANE, KHALOUFI, 2018). In addition to all the possibilities that unveil in its implementation, there are situations such as of facing pandemics.

The COVID-19 pandemic anticipated a debate that should have been carried out and advanced over the past few years: what is the limit for relativizing the right to privacy in the face of calamities in the health field, knowing that access to personal and sensitive data from the population can assist in the prevention and real-time monitoring of the spread of infectious diseases?

This is the main discussion that arises in the legal field today, notably so that in the future government authorities are more prepared to take advantage of new technologies without fear of arbitrary violations of the right to privacy.

It is known that there are no absolute fundamental rights. From this premise, it is totally credible to admit the relativization of the right to privacy and protection of personal data in the face of adverse situations such as pandemics, that is, issues of health law intrinsically linked to the right to health.

Before entering the discussion itself, it is necessary to present some basic concepts, as well as to contextualize the moment in which humanity lives, notably in the face of the so-called Surveillance Society linked to a Surveillance Economy.

### 4.1. From the Surveillance Society to Liquid Vigilance: well-founded fears about sharing personal data and the right to privacy

Health certainly tends to weight more in cases of balancing interests involving the right to privacy. However, the moment humanity currently faces, consisting of a true technological revolution, capable of undermining the right to privacy if even minimal limitations are not imposed, cannot be denied.

Technological evolution has made it possible to build an “Economics of Surveillance that tends to position the citizen as a mere spectator of their information” (BIONI, 2020, p.12) through Big Data (organization of data in a more scalable way). The personal data of citizens has become extremely valuable assets for large corporations. Nowadays, the possession of large amounts of data means power.

In fact, through ample access to personal data it is possible for companies to seek to improve their own business, making use of such data, but concurrently negotiate it by giving access to other corporations. In addition, the internet user is always being monitored, leaving "digital footprints" where one navigates, which are used to target advertising in a personalized way. Social networks also appear as a great ally in this constant monitoring. It is in this gray layer that most problems related to privacy and data protection arise.

As a result, several regulatory data protection frameworks have emerged around the world, the European one being the best known (EU Regulation 2016/670

of the European Parliament and of the Council of the 27th of April 2016), which was used as a model for the preparation of the General Data Protection Law in Brazil.

Therefore, the main concern that arises is the misuse of data by both companies and governments, without the consent of the citizen, transforming him into a true citizen or man of glass (transparent and without any secrets to be preserved (RODOTÁ, 2008, p.47). In this context, data brokers appear, and as Bruno Bioni affirms:

> It is an industry capable of gathering pieces of information from numerous sources, public (governmental) and private (acquired from the private sector) databases, which are not restricted to the online environment, in order to sell and resell citizens' personal data. The prefix 're', which denotes the repetition of an activity, emphasizes the outstanding characteristic of this industry, which is to extract the maximum profitability from this surveillance economy (BIONI, 2020, p. 27).

However, such a Surveillance Economy develops itself in the context of the Surveillance Society. The Surveillance Society presupposes such a continuous social control through new technologies (e.g. Big Data, drones, facial recognition). As Stefano Rodotá highlights:

> The innovation is radical. The risks of the surveillance society have traditionally been linked to the political use of information to control citizens, which qualifies such societies as authoritarian and dictatorial. In the perspective that is being outlined, on the contrary, the idea of vigilance invades every moment of life and presents itself with a characteristic of market relations, whose fluidity concerns the possibility of freely having a growing set of information. This materializes the image of the 'glass man', the true citizen of this new world. An image that, as it is no coincidence, comes directly from the time of Nazism, and that proposes a profoundly altered form of social organization, a kind of unstoppable transformation of the 'information society' into 'surveillance society' (RODOTÁ, 2008, p. 113).

In fact, the real objective in such surveillance society is classification, gradually revealing itself as a classification society (RODOTÁ, 2008, p.114). For Bauman, contemporaneity within the context of liquid modernity[8] presents the concept of liquid surveillance. For the author, we live in a moment when everything that is solid falls apart in the air, that is, all social forms fall apart faster than the speed with which new forms are created. "They cannot maintain their mold or solidify into reference frameworks for human beings' actions and life strategies due to the brevity of their own useful life" (BAUMAN, 2014, p. 7).

[8] To further knowledge, see BAUMAN, MODERNIDADE LÍQUIDA, 2001.

Therefore departing from the concept of solid surveillance of the panopticon idealized by Jeremy Bentham and, subsequently perfected by Michel Foucault, one should start, as did Gilles Deleuze, with the concept of a control society that grows not as a tree, but as a weeds (BAUMAN, 2014, p. 7). From here on, the idea of liquid surveillance can be understood, since the "inspector" does not stand behind the panopticon but can now slip through unreachable domains. For Bauman, consequently, we are faced with the post-panoptical era:

> Panoptic is just one surveillance model. The architecture of the electronic technologies by which power asserts itself in today's changing and mobile organizations makes the architecture of walls and windows largely redundant (despite firewalls and windows). And it allows forms of control that have different faces, that do not have an obvious connection with imprisonment and, moreover, often share the characteristics of flexibility and fun found in entertainment and consumption (BAUMAN, 2018, p. 8).

The new technologies thus give a false impression of freedom, imprisoning citizens in a much more effective way, through constant but dynamic surveillance that is constantly being reshaped.

Unlike the solid surveillance that consolidates the power of surveillance in a solid figure like the Big Brother of Orwell (BIONI, 2020, p. 133)[9], the liquid surveillance is diluted by the multiplication of Little brothers, in the face of an economy of surveillance in which its actors have as a business model to monitor the potential consumer citizens (BIONI, 2020, p. 135). Orwell's telescreen is replaced by countless microscreens, from smartphones to trackers[10], in a continuous surveillance architecture (BIONI, 2020, p. 135).

These considerations clearly demonstrate what are the risks and tensions generated from this change in the "surveillance" model that, based on new technologies, puts citizens in clear evidence, completely exposing them to the whole society in all aspects of their life. As a result, the protection of privacy and intimacy is increasingly reduced.

Having established the context in which the theme of privacy and protection of personal data is developed, we will now proceed to address the possible limits

[9] George Orwell wrote the dystopic romance "1984". The protagonist Winston was able to sometimes escape from the surveillance of the Big Brother. The telescreen was a type of bidimensional technology used much like a television to transmit the official government messages and sometimes, also used as a surveillance camera to observe citizens in their residences.

[10] Refers to all consumption habits tracking tools through one's navigation in the internet, such as cookies.

regarding the flexibility of its access, even in the face of health issues.

### 4.2. Privacy and sensitive data protection as fundamental rights

The birth of privacy is historically associated with the breakdown of feudal society, in which individuals were linked by a series of relationships that were reflected in the organization of daily life, that is, “isolation was the privilege of very few elected or those who, out of necessity or option, lived far from the communities” (RODOTÁ, 2008, p. 26). In that way, privacy rises as a possibility for the bourgeois class, who manages to achieve it due to the socioeconomic changes resulting from the Industrial Revolution. In fact, privacy arises "as the acquisition of a privilege by a group" (RODOTÁ, 2008, p. 27).

However, the right to privacy or originally the "right to be alone" should not be treated as elitist. Currently, this concept presumes greater complexity, reaching the status of a fundamental constitutional law in the West. The use of privacy under an elitist baton has therefore gone from opposing the provision of information to the State to enable social interventions; for an opposition to the granting of personal information as a reaction to authoritarianism and against a policy of discrimination based on political opinions (RODOTÁ, 2008, p. 30). In this sense, Stefano Rodotá highlights:

> Thus, privacy becomes a way of promoting parity of treatment among citizens, of achieving equality and not of protecting privilege, breaking its connection with the bourgeois class (RODOTÁ, 2008, p. 30).

Privacy evolves beyond the “right to be alone” in order to also involve the individual's right to maintain control over one’s personal data. Data appear in this context initially as elements of privacy, but quickly adopt an extremely relevant role as an autonomous right to protect personal data.

Furthermore, as Regina Linden Ruaro, Daniel Piñero Rodriguez and Brunize Finger point, the need to recognize the individual's right to control the information that concerns them, but also to limit the use and conservation of their data in public and private archives, were essential to highlight the need to create new frontiers appropriate to the digital reality, and, specifically, for the protection of personal data. That is why, in the authors' view:

> In a prospective view, there must be a state concern in order to germinate

> the perception that, as individuals and as a society, in the face of the digital dimensions now existing, living in a democratically organized social group assumed another meaning, and this includes, first of all, the clear notion of what it actually means to disseminate information today. To the same extent, it is important that there is adequate protection in the face of its records, distortions, and manipulations. This is a crucial task in the information society, but it is too neglected by states (RUARO, RODRIGUEZ, FINGER, 2008, p. 47).

It follows that the fundamental right to privacy constitutes a negative freedom against state action and seeks to preserve the right to privacy, freedom of decision on the disclosure of their information and the autonomy of each citizen. On the other hand, the fundamental right to the protection of personal data originates subsequently from the right to privacy. It is the result of the so-called information society that denotes the intrinsic power of those who display a large amount of personal data at their disposal. The right to protection of personal data is much broader than the right to privacy, as it is the positive freedom required of the State, that is, the State must act to guarantee the protection of personal data, through its own regulation, removing and avoiding potential violations of the rights to equality, freedom and non-discrimination. Even with the publication of the data by the individual, the individual will still have the right to control his or her personal data (VERGILI, 2019).

It is important to emphasize that the data is the primitive state of information, as it is not something *per se* capable of adding knowledge (DONEDA, 2006, p. 152). “Data are simply raw facts that, when processed and organized, become something intelligible, allowing some information to be extracted from it” (BIONI, 2020, p. 31-32).

The application of information technologies using algorithms to extract information from a massive amount of data collected by the government or private entities presents itself as the new danger to the violation of privacy and personal data, dealing with the last true extensions of one's personality. It is no wonder that, in addition to defending the fundamental right to the protection of personal data, personal data is also currently considered as a category of personality rights (BIONI, 2020, p. 56-57).

Precisely for this reason, faced with a scenario of tension or collision between the fundamental right to privacy as opposed to the necessary protection of the collective good (in this case of health), it is necessary that the fundamental rights in question be compatible. Certainly, the choice between which of fundamental rights should prevail should be based on the analysis of the specific case, but mainly from

the precepts established by the principles of proportionality and reasonableness, which are used as a mechanism for "weighting" fundamental rights apparently in collision.

In this particular, despite the criticisms that can be pointed out about possible subjectivism in the theoretical formulation of the weighting (after all, the weighting will represent an act of choice of the judge, which can be based on a subjective criterion, as warned by STRECK, 2014), the collision between the protection of collective health and the right of privacy should be resolved through the technique of weighting.

In this sense, Robert Alexy (ALEXY, 2008) argues that the collision between fundamental principles or rights must be resolved by means of a "conditional precedence relationship", that is, from the specific circumstances of each specific case, conditions should be laid down which will assign different weights to colliding rights and allow their prevalence. In this case, the idea of "all or nothing" will not apply, as proclaimed by Ronald Dworkin (DWORKIN, 1989), since in the case of a "collision" between fundamental principles or rights the temporary removal of the one that was preceded does not imply the need for his purge of the system.

The technique of "weighting" of alexyana matrix has been applied to the resolution of so-called hard cases, it is worth saying, those in which the mere subsumption of the fact to the norm does not show itself as sufficient. In this regard BARROSO (2009, p. 334) states that the weighting "is a technique of legal decision, applicable to difficult cases, in relation to which the subsumption proved insufficient". This process of applying the "weighting" technique can be summarized in three steps, namely:

> In the first step the interpreter should detect in the system the rules applicable to the specific case (higher premises), group them according to the solution they are suggesting and identify possible conflicts between them. In the second stage, the right applier should pay due to the technical examination of the question to its interpretation and to the reflections that the previously detected norms may point out when converged to concrete situations. In the third and final phase, where the singularization of the interpretative process and the application of the weighting are perceived, the larger dissonance assumptions and the repercussion of the specific case will be examined together, so that the various elements can be weighed in the problem and indicate which group of norms should prevail in the case (GUNDIM, 2015, p. 15).

The guiding thread of this whole weigh up process is based on the principle of proportionality, which must be analyzed in each specific case from the dimensions of

adequacy, necessity and proportionality in the strict sense (ALEXY, 2012). When dealing with the dimensions in question, Virgílio Afonso da Silva (SILVA, 2002) summarizes them as follows: 1) adequacy: it is considered as appropriate not only the mechanism that allows to achieve a certain objective, but also the one whose use promotes the promotion and promotion of a given objective. This has important implications because otherwise a measure can only be considered inadequate if its use cannot contribute to encourage the achievement of the desired objective; 2) need: the limitation of a fundamental right can only be considered as necessary in cases where the achievement of the objective cannot be effected, with the same intensity, by another mechanism that does not affect in the same way the fundamental right that will be achieved; and 3) proportionality in the strict sense: it is not enough that a measure of limitation to a fundamental right is taken as adequate or necessary, since it is also necessary to carry out a "restriction between the restriction of the fundamental right reached and the importance of the realization of the fundamental right that it controls and which underlies the adoption of the restrictive measure" (SILVA, 2002, p. 39).

## 5. SENSITIVE PERSONAL HEALTH DATA AND THE LIMITS TO ITS USE IN THE CONTEXT OF THE FIGHT AGAINST COVID-19 IN BRAZIL

Some data are considered to be sensitive. These "are a kind of personal data that comprise a different typology because its content offers a special vulnerability: discrimination" (BIONI, 2020, p. 83).

These are data related to sexual, religious, political, racial, health status or union membership[11]. The categorization into sensitive personal data denotes the discriminatory potential that such data can have if accessed and used for the most diverse purposes. Therefore, in order to guarantee respect for the principle of equality in treatment, personal data protection laws, including the Brazilian law, dedicate their own legal regime that is more protective regarding sensitive data.

Sensitive data have an objective protection aspect, but also deal with a subjective aspect, consistent of the fact that the citizen himself makes public some of

[11] The General Data Protection Law - GDPL in Brazil provides the definition of sensitive data in its art. 5, II: “sensitive personal data: personal data about racial or ethnic origin, religious beliefs, political opinion, union membership or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person” (LGPD, 2020).

his sensitive personal data. Even in these cases, it is the citizen's choice to exercise his fundamental right to data protection.

Among the various sensitive data, health data are significant for the purposes of this study (ABOUELMEHDI, BENI-HESSANE, KHALOUFI, 2018, p. 4)[12]. The premise that must be established is that there is a possibility of coexistence between the protection of sensitive data and the collection or treatment of that data in the face of extraordinary situations, such as the health crisis provided by COVID-19. However, the relevance of the security of sensitive data is highlighted throughout the entire cycle, from collection and treatment to its disposal[13].

There is no international legislation that unifies data processing. Each country has its own legislation, which is why the issue is challenging. However, health data is noteworthy, since they can be collected by the government as a way of monitoring and controlling the spread of infectious diseases, even temporarily.

It happened before in South Korea in 2015 with the outbreak of Mers (an Asian epidemic of another coronavirus), but the government was not transparent in collecting, hiding it, precisely in face of privacy protection. Such a position was widely criticized, which is why major legislative reforms were advanced regarding the sharing and public management of information about patients with infectious diseases. The 2016s Personal Information Protection Act excluded the need for consent, limitations and guarantees regarding personal data when information was temporarily required and urgent for safety, well-being and health (SOUTH KOREA, 2011).

When analyzing the behavior of South Korea in the fight against COVID-19, it appears that its preventive and monitoring actions, based on the mentioned legislation, provided one of the best governmental responses to the virus. Certainly,

[12] Abouelmehdi, Beni-Hessane & Khaloufi, *supra* note 42, at. 4. "Security and privacy in big data are important issues. Privacy is often defined as having the ability to protect sensitive information about personally identifiable health care information. It focuses on the use and governance of individual's personal data like making policies and establishing authorization requirements to ensure that patients' personal information is being collected, shared and utilized in right ways. While security is typically defined as the protection against unauthorized access, with some including explicit mention of integrity and availability. It focuses on protecting data from pernicious attacks and stealing data for profit. Although security is vital for protecting data but it's insufficient for addressing privacy".

[13] "[...] that security in big data refers to three matters: data security, access control, and information security. In this regard, healthcare organizations must implement security measures and approaches to protect their big data, associated hardware and software, and both clinical and administrative information from internal and external risks. At a project's inception, the data lifecycle must be established to ensure that appropriate decisions are made about retention, cost effectiveness, reuse and auditing of historical or new data" (ABOUELMEHDI, BENI-HESSANE, KHALOUFI, 2018, p.5).

the great transparency that has been given to the data exposes the contaminated population, even though it uses the so-called aggregated data with anonymity, since it is known that despite the authorities ensuring that the data is anonymous, it appears to be public and notorious that the reversal of anonymization is always possible. This possible reversal is called the "mosaic effect", as it allows several pieces of data to be aggregated in order to reveal the puzzle image, previously disfigured (BIONI, 2020, p.65). In this model, South Korea has stipulated all individuals as monitoring recipients, generating true self-protection.

In view of this situation, the General Data Protection Law - GDPL in Brazil (Law No. 13.709 / 2018), which will be enforced as of August 2020, is clear in its art. 11 that sensitive personal data, including health data, can be processed regardless of the consent of the holder, when indispensable for the implementation of public policies provided for in laws and regulations involving the protection of life, the physical safety of the holder, or of third parties, as well as to the exclusive protection of health, in a procedure performed by health professionals, health services or health authority (EHRHARDT JUNIOR, MODESTO, 2020, p. 9).

Initially, in facing exceptional situations such as the COVID-19 pandemic, there are no questions about the collection and treatment of sensitive data. However, such collections and treatments cannot be indiscriminate, that is, they must respect limits. Although the LGPD is yet not being enforced, some basic principles contained in the Law, which can also be subject to extraction from the constitutional arrangement itself, constructions of doctrine or jurisprudence, deserve observation. These are the principles of purpose, necessity, as well as reasonable deliberation in data processing.

Any sensitive data collection by the government, therefore, must be guided by an objective, that is, its purposes must be legitimate and specific, in order to avoid or repress further treatment incompatible with the initially motivating purpose. Thus, there must be adequacy, consistent with the compatibility of the treatment with the initial purposes. In addition, there must be a need in the treatment of such data, that is, one should not extrapolate the scope of the data collected beyond what is strictly essential for the purpose set. Finally, the regarding the owner of sensitive data must be wide, under penalty of liability at any stage of the chain of treatment of such data.

However, it is important to highlight that several new technologies are emerging to ensure security and privacy even when using sensitive data by Big Data

Health, such as authentication tools, encryption, data masking and access control[14].

Having exposed the current concerns that accompany the subject of personal data protection and its respective limits, we begin to analyze the treatment given to personal data as an instrument to combat COVID-19 in Brazil.

### 5.1. Technology and sensitive data protection in the COVID-19 context in Brazil

In Brazil, the federative republic is presented as the basis of the system founded on the principle of separation of powers and on the constitutional basis of political pluralism. Thus, the western democratic character present in Brazil ultimately highlights privacy as a fundamental right. Allied to this, as already mentioned, there is the GDPL elaborated in the light of the General European Data Law[15]. Therefore, limits are imposed, as well as parameters and the necessary observance of principles when processing personal data, with special attention to the so-called sensitive data, with health data standing out among these.

In Brazil, some technologies were used to monitor and control the pandemic, but in a more tenuous way. In the State of São Paulo, as of mid-April 2020, it was determined by the Government through State Decree nº 64.936 / 2020 (BRASIL, 2020) that personal telephone data would be treated, notably for the purpose of monitoring compliance with isolation measures[16], based on the geolocation system (G1 SP, 2020). This initiative by the State Government took place through the establishment of a cooperation called the Intelligent Monitoring System (SIMI-SP) between the telephone operators Vivo, Claro, Oi and Tim, Brazilian Association of Telecommunications Resources (ABR) and the Technological Research Institute (IPT[17]), which enabled the State to consult anonymous aggregated information on displacement in mapped São Paulo municipalities (SECRETARIA DE DESENVOLVIMENTO ECONÔMICO, 2020).

In Amazonas, for example, the state government decreed a quarantine regime

[14] To further knowledge, see Abouelmehdi, Beni-Hessane & and Khaloufi.
[15] EU Regulation no. 2016/679 of 27 April 2016 (European General Regulation for the Protection of Personal Data - GRPD).
[16] Decree No. 64,936 / 2020 was challenged in court due to the fear of misuse of personal data. However, the special body of the Court of Justice of the State of São Paulo, on June 8, 2020, decided by majority of votes that there is no illegality in the monitoring resulting from the cooperation term signed by the Government of the State of São Paulo, since personal data would not be used, only aggregated anonymous data.
[17] See Extracts from the Cooperation Terms (30 Jun 2020), https://www.ipt.br/noticia/1612-acoes_emergenciais_no_combate_ao_covid_19.htm.

for those who disembarked at Eduardo Gomes International Airport. It also developed an application for smartphones to be installed by all passengers, which works as a real-time location monitor during the 14 days people are submitted to quarantine (EHRHARDT JUNIOR, MODESTO, 2020, p.10). In Recife, in turn, the municipality also used the system of geolocation of cell phones to coordinate actions in order to encourage social isolation (G1 PE, 2020).

The Ministry of Science, Technology, Innovations and Communications highlighted some measures that have been taken in Brazil, such as the monitoring of cases and the printing of protective masks using 3D printers (MCTIC, 2020).

In the city of São Paulo, the use of ultraviolet (UV) equipment to sanitize the train cars that circulate in the subway is being tested. If the results are positive, there is a possibility of its extension to the entire state transport system (PORTAL DO GOVERNO, 2020). Still in São Paulo, some hospitals have been using "UV-C squeegees" to decontaminate the floor; air conditioning filtration systems, as well as tele-presence robots to screen patients, preventing the spread of the disease to health professionals (UOL, 2020).

Therefore, Brazil has made use of certain technologies, but the closest the country came to the collection and processing of personal data was the monitoring of smartphones for the purpose of measuring the percentage of social isolation.

The Federal Government tried, via decree, to share telephone data to serve as a database for study purposes by the Brazilian Institute of Geography and Statistics – IBGE (IBGE, 2020). However, the indicated rule had its effectiveness suspended in an injunction granted by the Supreme Federal Court, in view of the violation of basic principles such as purpose, necessity, reasonableness and proportionality (STF, 2020).

A platform called "Together against COVID" was recently launched to assist in the tracking of COVID-19 cases in Brazil. It is a non-governmental initiative, through which citizens voluntarily fill out online forms indicating whether they have symptoms or have had contact with those infected by the disease. It is then possible to research the estimated contamination risk of COVID-19 by region[18]. It is a self-protection measure that comes close to the South Korean experience, but which did not have state initiative, which is why it could have been much more effective.

[18] See Together Agains COVID (27 May 2020), https://www.juntoscontraocovid.org/.

In combating possible new pandemics in the future, China's experience can bring important contributions to be considered. The use of drones for delivery in extremely affected locations and artificial intelligence and Big Data with the improvement of monitoring are presented as viable technological options. The use of artificial intelligence for the sanitization of public places and parks is also a fully applicable measure.

The creation of a governmental platform that ensures the anonymization of data, as well as its safe disposal after the end of the pandemic, combined with the use of QR codes that involve sensitive data does not present itself as a violation of privacy, provided they are used observing the principles of purpose, adequacy, necessity, reasonability and proportionality,. It is enough to analyze the non-governmental platform initiative that already tracks COVID-19, which has massive citizen participation, to verify the possibility of considering such an official government mechanism in the future.

Several countries have made use of mobile applications called contact tracing (ALMEIDA et al., 2020, p. 2488)[19], using heat maps so that the population can become aware of infected individuals around them and take the appropriate precautions. There is a great debate in Europe about which is the best contact tracing model, that is, the option between the centralized and the decentralized model. In the centralized model, all data is sent to a central server that triggers notices to the cellphones of those potentially infected. In the decentralized model, Bluetooth technology is applied among cellphones and the transmission of the ID occurs between the smartphones that download the information themselves, allowing citizens to learn or not about possible contact with infected people[20]. In this case,

[19] "Apple and Google recently entered into a partnership, aimed at ensuring interoperability between iOS and Android systems, for the creation of a tracking tool for COVID-19. According to the companies, people will have the option to participate, no mention is made to the option of withdrawing consent at any time. The system, according to published specifications6, has similarities with solutions that have been referred to as 'contact tracing' and are inspired, broadly, by implementation already operational in Singapore and proposals under development in Europe such as DP-3T (Decentralized Privacy-Preserving Proximity Tracing) or the PEPP-PT (Pan-European Privacy-Pre-serving Proximity Tracing) project. This proposal, like MIT's Safe Paths Platform, seeks to maximize privacy" (ALMEIDA et al., 2020, p. 2488).

[20] "When a person has a positive result for the coronavirus, this registration will be made in the application, which will be transmitted to health authorities in their respective country. Then, people with whom you have had contact in the previous 14 days will be alerted that they have been in contact with someone who has been diagnosed positive for the disease. As these are technologies are still in the development and maturation phase, there are differences between implementations that, over time, can prove to be very significant, as, for example, it already seems to be the centralized focus of the PEPP-PT in contrast to the decentralized one DP-3T " (ALMEIDA et al., 2020, 2488).

there is no central server, which results in greater protection for privacy and personal data.

Certainly, both geolocation tracking or monitoring and contact tracing deal with what Stefano Rodotá calls “electronic rattles” (RODOTÁ, 2018, p. 252) and point to a type of surveillance determined by the government. However, in situations of extreme urgency and necessary temporary social control, it must be acceptable, precisely to avoid the spread of infectious diseases and the preservation of health and life. The situation must be guided by the supremacy of the public interest over the private one in exceptional moments. But that does not exclude a weighting of values that, while protecting health and life, also guarantees the postulates of privacy and protection of personal data. Responsible governance must be guided by transparency in the collection and processing of data and the purposes assigned to them.

As it is well highlighted by Almeida *et al*:

> Proper, responsible, and sustainable data governance models, which protect and defend ethical and regulatory principles, increase the confidence of individuals and society in the use of their data to respond to situations of legitimate public interest. Aspects related to the right to privacy, the right to the protection of personal data and the rights of groups do not prevent the use of personal data and the possibility of their use to respond to the pandemic. The public health emergency caused by Sars-CoV-2 points to the pressing need for new forms of personal data governance that include civil society to promote equitable benefits for society as a whole (ALMEIDA et al., 2020, p. 2491).

Caution will certainly never be excessive, so no abuse is perpetuated harmful effects in the long run are caused[21]. This is one of Yuval Noah Harari's biggest fears (HARARI, 2020)[22]. The use of facial recognition and surveillance cameras that

[21] “Concerns about privacy and data protection. Governments in China, South Korea, Israel and elsewhere have openly accessed and used personal mobile phone data for tracking individual movements and for notifying individuals. However, in other regions, such as in Europe, both national and regional legal regulations limit such use (especially the European Union law on data protection and privacy known as the General Data Protection Regulation - GDPR). Furthermore, around the world, public opinion surveys, social media and a broad range of civil society actors including consumer groups and human rights organizations have raised legitimate concerns around the ethics, potential loss of privacy and long-term impact on civil liberties resulting from the use of individual mobile data to monitor COVID-19 and send personalized notifications to citizens” (OLIVER et al., 2020, p. 8).

[22] The pandemic can now justify surveillance, but after it is possible that the maintenance of frightening surveillance will be legitimized. The danger is that now you no longer monitor only the links and ideological positions, but rather the body temperature, joy, sadness as you watch a movie, propaganda, etc. and this can be used by large corporations. Biometric monitoring can make the Cambridge Analytical episode look like the Stone Age. And data-hungry governments may want to extend the need for biometric monitoring precisely on the basis of a possible second wave of viruses, for example. And if the population has to choose between maintaining privacy or protecting health, will

capture the body temperature of citizens without their consent, for example, are Chinese practices that are open to question for use in Brazil. The Brazilian democratic tradition linked to its mirroring in the European data protection legislation removes these more invasive control modalities.

## 6. FINAL CONSIDERATIONS

The COVID-19 pandemic has brought valuable lessons to humanity. First, it gave greater visibility to the glaring inequalities in the countries of the global south, notably regarding the need for public policies on health, education, and basic sanitation. Thus, at first the virus leaves the need for strengthening the role of the State in providing efficient and quality public services to combat future pandemics as an initial pedagogy.

In addition, it demonstrated that the available technologies can and must be used to fight infectious diseases. This study demonstrated the important role of Big Data in the treatment of sensitive personal health data in the task of monitoring and fighting the virus. It was also possible to verify the dangers of the collection and processing of sensitive personal data by the government in a surveillance society.

In fact, Bauman's concept of liquid surveillance has never been more actual. However, it is possible to make privacy more flexible without neglecting the protection of personal data, making use of necessary weighting of values in exceptional situations, such as the pandemic of COVID-19. The observance of principles such as necessity, purpose, reasonableness and proportionality, in addition to the imposition of good governance based on transparency and ethics, are essential elements for the protection of sensitive personal data, as well as to solidify the population's confidence in governmental actions at times crisis.

Many countries have adopted monitoring measures by geolocation and contact tracing as ways to track and prevent the spread of the disease among the population. Brazil has adopted monitoring in some Member States, such as São Paulo, but the measures were tenuous. For the future, there is a need to adopt monitoring and/or contact tracing models from countries that have had successful experience such as South Korea, China and Germany, through the use of the

always choose the latter (HARARI, 2020).

decentralized model, which guarantees greater protection to privacy. The provision of the self-declaration option in cellphone applications for the purposes of feeding the government's official monitoring programs is also an alternative that preserves consent and control over the citizen's own data and at the same time cooperates to contain the dissemination of the disease.

Thus, although the supremacy of the public interest over the private one prevails in situations of calamity and emergencies, it has to be said that it is not an absolute concept, that is, in extreme situations regarding the protection of sensitive personal data, it is necessary to observe limits for its flexibilization, based on principles and on the essential regulatory legal framework in Brazil with the General Data Protection Law - GDPL.

## REFERENCES

ABOUELMEHDI, Karim; BENI-HESSANE, Abderrahim; KHALOUFI, Hayat. Big healthcare data: preserving security and privacy. **Journal of Big Data**, p. 1-18, 2018.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgilio Afonso da Silva. São Paulo: Malheiros Editores, 2008.

ALMEIDA, Bethania de Araujo et al., Personal data usage and privacy considerations in the covid-19 global pandemic, **CIENC. E SAUDE COLETIVA**, p. 2487–2492, 2020.

BANSAL, Shweta; CHOWELLI, Gerardo; SIMONSEN, Lone; VESPIGNANI, Alessandro; VIBOUD, Cécile. Big Data for Infectious Disease Surveillance and Modeling. **The Journal of Infections Diseases – JID**, pp. S375-S379, 2016. Disponível em: http://jid.oxfordjournals.org/. Acesso em: 21 maio 2020.

BARROSO, Luis Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009.

BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

BAUMAN, Zygmunt. **Modernidade líquida.** Ed. Zahar, 2001.

BENKLER, Yochai. Technology, law, freedom and development, **Indian Journal of Law and Technology 1**, no. Issue (2005): 1-14.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020.

BOULOS, Maged N. Kamel; GERAGHTY, Estella M. Geographical tracking and

mapping of coronavirus disease COVID-19/severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics. **International Journal of Health Geographics.** 2020.

BRASIL. LGPD**. Lei nº 13.709, de 14 de Agosto de 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 26 maio 2020).

BRASILa. **Medida Provisória n. 954, de 17 de abril de 2020**. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 27 maio 2020.

BUCKEE, Caroline. Improving epidemic surveillance and response: big data is dead, long live big data**. Lancet Digital Health**. March, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DWORKIN, Ronald. **Los derechos en serio**. 2 ed. –Barcelona: Ariel, 1989.

EHRHARDT JUNIOR, Marcos; MODESTO, Jéssica Andrade. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Redes: Revista Eletrônica Direito e Sociedade**, Canoas, v. 8, n. 2, Ahead of print, ago. 2020.

G1 PE. **Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus**. 24 mar. 2020. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-paramonitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml. Acesso em: 27 maio 2020.

G1 SP. **SP usa sistema de monitoramento com sinais de celulares para localizar aglomeração de pessoas no estado**. 09 de abr. 2020. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/04/09/sp-usa-sistema-de-monitoramento-com-sinais-de-celulares-para-localizar-aglomeracao-de-pessoas-no-estado.ghtml. Acesso em: 27 maio 2020.

GUNDIM, Wagner Wilson Deiró. Hidras e Hércules: a relação circular entre princípios e regras. **Revista da Faculdade de Direito de São Bernardo do Campo**, v. 21, n. 2, 2015. Disponível em: https://revistas.direitosbc.br/index.php/fdsbc/article/view/793.

HARARI, Yuval Noah. **The world after coronavirus**. Financial Times, 2020.

KAYES, A. S. M.; ISLAM, Saiful; WATTERS, Paul A; NG, Alex; KAYESH, Humayun. Automated Measurement of Attitudes Towards Social Distancing Using Social Media: A COVID-19 Case Study. **Preprints.** 2020.

MCTIC. **Ações de combate a covid-19 são destaques do MCTIC nos 500 dias de**

**governo.** 15 maio 2020. Disponível em: http://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2020/05/Acoes_de_combate_a_covid19_sao_destaques_do_MCTIC_nos_500_dias_de_governo.html. Acesso em: 27 maio 2020.

MIIT. **Ministry of industry and information technology of the people's Republic of China.** 2020. Disponível em: http://www.miit.gov.cn. Acesso em: 20 maio 2020.

OLIVER, Nuria; LETOUZ, Emmanuel; STERLY, Harald; DELATAILLE, S´ebastien; NADAI, Marco De; LEPRI, Bruno; LAMBIOTTE, Renaud; BENJAMINS, Richard; CATTUTO, Ciro; COLIZZA, Vittoria; CORDES, Nicolas de; FRAIBERGER, Samuel P.; KOEBE, Till; LEHMANN, Sune; MURILLO, Juan; PENTLAND, Alex; PHAM, Phuong N.; PIVETTA, Frdric; SALAH, Albert A.; SARAMKI, Jari; SCARPINO, Samuel V.; TIZZONI, Michele; VERHULST, Stefaan; VINCK, Patrick. Mobile phone data and COVID-19: missing an opportunity*?* **arXiv preprint arXiv**:2003.12347, 2020.

PORTAL DO GOVERNO. **Transportes metropolitanos testa tecnologia para combate ao Covid-19.** 16 abr. 2020. Disponível em: https://www.saopaulo.sp.gov.br/noticias-coronavirus/transportes-metropolitanos-testa-tecnologia-para-combate-ao-covid-19/. Acesso em: 27 abr. 2020.

PUGLIESI, Márcio, BRANDÃO, André. Uma conjectura sobre as tecnologias de Big Data na prática jurídica. **Rev. da Fac. Direito da UFMG**, p. 453–482, 2016. DOI: 10.12818/P.0304-2340.2015v67.

RODOTÁ, Stefano**. A vida na sociedade da vigilância** – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden, RODIGUEZ, Daniel Piñeiro, FINGER, Brunize. **O direito à proteção de dados pessoais e a privacidade**, pp. 29–64, 2008.

SANTOS, Boaventura de Sousa. **A cruel pedagogia do Vírus***.* Coimbra: Almedina, 2020.

SCHWAB, Klaus. **A quarta revolução industrial**. 1 ed. Edipro: 2016.

SHAW, Rajib; KIM, Yong-kyun; HUA, Jinling. Governance, technology and citizen behavior in pandemic: Lessons from COVID-19 in East Asia. **Progress in Disaster Science** 6. 2020.

SILVA, Virgílio Afonso da. O proporcional e o razoável. **Revista dos Tribunais**, n. 798, 2002. Disponível em: https://constituicao.direito.usp.br/wp-content/uploads/2002-RT798-Proporcionalidade.pdf. Acesso em: 10, ago. 2021.

SOUTH KOREA. **Personal information protection Act.** 29 mar. 2011. Disponível em: https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830758&leSn=1&nttId=8186&toolVer=&toolCntKey_1= Acesso em: 27 maio 2020.

STRECK, Lenio. **Lições de crítica hermenêutica do direito**. Porto Alegre: Livraria do Advogado Editora, 2014.

SUPREMO TRIBUNAL FEDERAL. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE.** 07 maio 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902. Acesso: 27 maio 2020.

UOL. **Hospitais buscam na tecnologia soluções para prevenir que covid se espalhe.** 24 abr. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/24/hospital-de-sp-filtra-ar-de-quartos-para-impedir-contaminacao-por-covid-19.htm. Acesso em: 27 maio 2020.

VERGILI, Gabriela Machado. Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados, **Dataprivacy**, 2019.

Recebido em 27/12/2020
Aprovado em 30/08/2021
Received in 12/27/2020
Approved in 08/30/2021