Personal Data Protection And Its Restrictions: A Reflection In Times Of Pandemic[1]

Proteção De Dados Pessoais e Suas Restrições: Uma Reflexão Em Tempos De Pandemia

Regina Linden Ruaro[2]

Abstract

This article proposes to present considerations about the appropriateness of restrictions to the fundamental right to personal data protection when faced with a situation of a dystopian scenario such as the SARS-CoV-2 Pandemic. After, it faces the situations and limits to the treatment and use of personal data by the Government and the private sector based on some fundamentals, principles and rules of the General Law for the Protection of Personal Data (Law nº 13.709/2018) and the Access to Information Law (Law nº 12.527/2011), with the legislative set that supports them based on Complementary Law nº 101 of 05/04/2000, and the Fiscal Responsibility Law, as amended by Complementary Law nº 131 of 05/27/2009, and also by Law nº 14.129/2021, which provides for principles, rules and instruments for Digital Government, as well as the regulatory set that is subsidiary and complementary to it.

Keywords: Access to Information. Pandemic. Personal Data Protection. Transparency.

[1] Recebido em: 10/4/2022. Aprovado em: 21/6/2022.

[2] Advogada e Consultora Jurídica nas áreas do Direito Administrativo, Direito Digital e da Proteção de Dados Pessoais. Professora Titular da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. Procuradora Federal/AGU aposentada. Doutora em Direito pela Universidad Complutense de Madrid (1993) com título revalidado pela UFRGS e Pós-Doutora pela Universidad San Pablo - CEU de Madri (2006/2008), Estágio Pós-doutoral na Universidade San Pablo - Ceu de Madri (2016) Compõe o Grupo Internacional de Pesquisa "Protección de Datos, Transparencia y Acceso a la Información". Coordenadora no Brasil pela PUCRS/PPGD/PUCRS no Projeto "Identidad Digital, Derechos Fundamentales y Neuroderechos" - Espanha. Professora convidada do Máster en Protección de Datos, Transparencia y Acceso a la Información da Universidad San Pablo de Madrid-CEU/ Espanha. Decana Associada da Escola de Direito (2018/2021), Membro do Comitê Gestor do Biobanco da PUCRS, Membro Honorário do Instituto Internacional de Estudos de Direito do Estado - IEDE. Lidera o Grupo de Pesquisa cadastrado no CNPq: Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação no Estado Democrático de Direito na linha de Direito, Ciência, Tecnologia e Inovação. Membro do Grupo do PPGD/PUCRS no Projeto HANGAR. E-mail: ruaro@pucrs.br.

Resumo

O artigo se propõe a apresentar considerações acerca do cabimento de restrições ao direito fundamental à proteção de dados pessoais quando se está frente a uma situação de um cenário distópico como a pandemia do SARSCOV-2. Após, enfrenta as situações e os limites ao tratamento e uso de dados pessoais pelo Poder Público e pela iniciativa privada com base em alguns fundamentos, princípios e normas da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e da Lei de Acesso à Informação (Lei nº 12.527/2011), com o conjunto legislativo que lhes dá sustentação e conexão normativa alicerçado pela Lei Complementar nº 101 de 04/05/2000, bem como pela Lei da Responsabilidade Fiscal, com a redação que lhe deu a Lei Complementar nº 131 de 27/05/2009, e ainda pela Lei nº 14.129/2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital, bem como o conjunto normativo que lhe é subsidiário e complementário.

Palavras-chave: Acesso à Informação. Pandemia. Proteção de Dados Pessoais. Transparência.

Introduction

The use of Information and Communication Technologies (ICTs) has caused and continues to cause many concerns, notably with regard to Personal Data Protection. This fact is currently relevant in view of the Pandemic scenario caused more than 02 (two) years ago by COVID-19, insofar as it has been causing a sharp traffic of data of the most diverse types. The epidemic has been affecting social relations in all sectors. The interests of all governments, whether national or international, are obviously centered on the hope of finding an effective solution that quickly combats the damage caused by the Pandemic that is ravaging the entire world. In this sense, the Federal Government of Brazil has been adopting measures that aim to further prevent the spread of the virus and, consequently, affect the fundamental rights and freedoms of all citizens.

In general and given the circumstances, this article seeks to demonstrate that, it is not possible, based on a plan, to delegitimize restrictions on freedoms, unless these are disproportionate and exceed the necessary time of containment, as well as the use to which they were willing to be helpful. Nevertheless, it is believed that in view of the Pandemic situation in the country, a more critical look at the protection of fundamental rights and freedoms, respectively, with a more

restricted focus from the point of view of personal data protection, is deemed necessary.

Therefore, although the obligations related to the processing of personal data should not, in any way, get tangled up or even prevent the saving of human lives, they should also not be forgotten or ignored for disproportionate reasons. The fact is that, as it involves personal data, there must be, above all, great care with the *relativization* of the rights of privacy and intimacy of citizenship.

One thing is clear: it is believed that the issue involving the protection of personal data is one of the most important from the point of view of the individual (data subject), especially in a situation where health data is involved, as these fall into the so-called category of sensitive personal data and, as such, benefit from enhanced protection. The misuse of this data, or its inappropriate and insensitive use, can also significantly affect the personal sphere of individuals in their social relationships and, thus, violate their right to protection of personality or privacy.

It is assumed that, in order to prevent inappropriate public reactions to any information (even those not yet confirmed), such as, for example, about the occurrence of possible worker illness as well as to prevent the possible opportunism of misuse, of that professional's data using the Pandemic situation as an excuse for the unauthorized collection of his/her personal data by public authorities (or even private companies), the issue of personal data protection, at least by the professional public (work related), should receive adequate attention. Informing the public about the course of the epidemic through the media is, undoubtedly, recommended, but it can also potentially involve the privacy of those affected by it, generating all kinds of discrimination.

It so happens that the collection and processing of personal data can be considered as important aspects used in the fight against the COVID-19 Pandemic. Besides that, it provides economic assistance, helps the national vaccination program and also aids the handling of issues related to the way people work during the Pandemic. This so happens because these collections serve the general interest of public and economic health, allowing decision-makers to act with full knowledge of the facts.

In fact, an attempt will be made to demonstrate that effective control of the Pandemic and providing the best possible protection to citizens against the SARS-CoV-2 virus would not be possible without the processing of personal data. Therefore, it is considered that the collection of such data must be allowed so that it can be analyzed, examined and evaluated with the main purpose of protecting the population. It is also of fundamental importance to define the best public health policy and, finally, the best economic incentives that should be provided to maintain that same health care with the least possible economic damage to private companies.

The article is aimed at analyzing the legality of the disclosure (processing) of personal data and information, on the Federal Government's Transparency Portal, regarding citizens who received the Emergency Financial Aid due to the Pandemic. Initially, in order to clarify the issue, this study is based on the CF (Brazilian Federal Constitution), in a systematic interpretation according to the LGPD, LAI and LGD[3], so as to demonstrate whether or not the disclosure made by the Public Power violated the personal data protection rights.

This reflection, evidently, does not intend to end the discussions on the subject, but intends to present considerations that aim to design situations and limits to the treatment and use of personal data by the Public Power and by the private initiative. All that based on some fundamentals, principles and rules of the General Law for the Protection of Personal Data, as well as other laws concerning the matter, which will be demonstrated throughout the article.

It is pointed out, previously, in consonance with the doctrine[4], that the fundamental right to privacy is not to be confused with the fundamental right to personal data protection, despite the fact that their relationship is undeniable, which is why the latter will also be treated as a right to “information privacy”.

This article is anchored in with line research on Law, Science, Technology & Innovation and in the Research Project, Protection of Personal

[3] BRAZIL, **Law nº 14.129 from March 29, 2021** –, which is called Digital Government Law (LGD). Available at https://www2.camara.leg.br/legin/fed/lei/2021/lei-14129-29-marco-2021-791203-norma-pl.html. Accessed on May 13, 2021.

[4] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. In: MENDES, Laura., DONEDA, Danilo., SARLET, Ingo. RODRIGUES JR., Otávio. (Org.) **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense. 2021. p. 32.

Data and Access to Information in the Democratic State of Law, of the Graduate Program in Law at PUCRS (Pontifical Catholic University of Rio Grande do Sul).

1.Personal Data Protection in Brazil: a recent fundamental right

After settling the previous premises and the contents necessary for the contextualization of the subject of study, it is necessary to address the fundamental right to personal data protection, a central point in the debate established in this article. Initially, it should be noted that privacy and personal data protection are distinct rights, despite the fact that there is a very significant relationship between the two of them. In this sense Sarlet, when dealing with the relationship between the right to personal data protection and the right to privacy [5], states that the relationship between the fundamental right to personal data protection and the right to privacy is not a complete superposition of the respective protection scopes and, likewise, the personal data protection and informational self-determination go beyond privacy and its protection, at least in the traditional sense of the term, being a logic of collection and exposure.

In turn, Bioni, when establishing a "dialogue" in relation to privacy and personal data protection, affirms […] "whichever is public and private is what regulates the content of the right to privacy, its logic being centered on the negative freedom of the individual not to be interfered with by others"[6] . Because of this dichotomy, the need to ensure a fundamental right to personal data protection is recognized, a right that has acquired extreme relevance from the emergence of ICTs since, due to broad technological progress, especially with the advancement of network computing, *ultima ratio* of Informatics, over the last decades, access and manipulation of information has been expanded, which led, among other factors, to the need for this right to exist specifically.

[5] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. In: MENDES, Laura., DONEDA, Danilo., SARLET, Ingo. RODRIGUES JR., Otávio. (Org.) **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense. 2021. p. 32.
[6] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais e os limites do consentimento**. p. 93.

In the Brazilian legal system, the Federal Constitution (CF), until very recently, did not express the terms of the fundamental right to personal data protection; the dogmatic construction about its fundamentality was based on doctrinal studies and the jurisprudence of the STF (Superior Federal Court). In this sense, when dealing with fundamental rights expressly in its article 5, item X, it provides for the right to intimacy and private life (privacy). Besides that, in item XII, it deals with the confidentiality of data communications and habeas data, in item LXXII.[7] Furthermore, Sarlet states that "the closest direct constitutional basis for a fundamental right to data protection is the free development of the personality"[8], wich the author calls "a general clause protecting all dimensions of the human personality"[9].

Even though there was no express provision in our constitutional text of the right to personal data protection, in the same way as in the EU Charter, Sarlet already considered it as a fundamental right that is associated with the right to privacy, provided for in article 5, item X, of the Brazilian Federal Constitution, and the right to the free development of personality, which includes the right to the free disposal of personal data. It should be noted that in our Federal Constitution (1988), a general personality right was not expressly conceived. However, the constitutional principle of the 'dignity of the human person' is revealed as a postulate that guarantees the protection of the personality and of the consequences attributed and invested by it. According to the author's lesson, the link between the right to privacy and the dignity of the human person is justified insofar as the preservation of a sphere of private life that is essential to the human

[7] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. In: MENDES, Laura., DONEDA, Danilo., SARLET, Ingo. RODRIGUES JR., Otávio. (Org.) **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense. 2021. p. 35.
[8] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. In: MENDES, Laura., DONEDA, Danilo., SARLET, Ingo. RODRIGUES JR., Otávio. (Org.) **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense. 2021. p. 36.
[9] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2019, p.169. Informational self-determination is understood by what Danilo Doneda teaches to be the fundamental right, as it is a right of personality, the individual has the power to control his/her own information.

beings' own mental health, ensuring the full development of their personality[10] and implying several legal positions[11].

Moreover, in the construction of a fundamental right to personal data protection, it was previously mentioned that the jurisprudence of the STF has an important and extremely topical factor. This understanding is based on the judgment of ADIn (Direct Action of Unconstitutionality) 6387 that regards to the monocratic decision by Minister Rosa Weber who, on 04/17/2020, granted an injunction, later confirmed by the STF Plenary, on 05/07/2020, to suspend the effectiveness of Provisional Measure No. 954/2020, which provided for the sharing of data from telecommunications users with the Brazilian Institute of Geography and Statistics (IBGE), under the pretext that such sharing was intended to produce official statistics during the Coronavirus Pandemic. In her vote, the Minister recognized that the information related to the identity of the natural person "constitute personal data and integrate, in this measure, the scope of protection of the constitutional clauses ensuring individual freedom (art. 5, caput), privacy and free development of the personality (art. 5, X and XII)[12].

The matter was overcome with the approval of PEC (Proposal for Amendment to the Constitution) 115/2022 which inserted in article 5 of the Federal Constitution, item LXXIX. It is important to point out the differential point that the personal data protection brings, which is the basis used both in doctrine and jurisprudence, in relation to the right to personality and its free development[13].

---

[10] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. In: MENDES, Laura., DONEDA, Danilo., SARLET, Ingo. RODRIGUES JR., Otávio. (Org.) **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense. 2021.

[11] The right of access databases; the right not to know, process, use and disseminate certain personal data by the State or by third parties; the right to know the identity of those responsible for the collection, storage, treatment and use of data; the right to know the purpose of the collection and eventual use of data and the right to rectification and delete personal data stored in a database. MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. **Curso de Direito Constitucional.** São Paulo: Revista dos Tribunais, 2014. p. 434/435.

[12] BRAZIL. Supremo Tribunal Federal (Plenary). **Referendum in Precautionary Measure in ADI 6.387/DF**. Reporter Minister Rosa Weber. May 7, 2020. Available at: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Accessed on April 20, 2021.

[13] It is not the objective of this study to discuss the concepts and theories about personality rights and their free development, however, it should be noted that Bruno Bioni's conception is adopted for whom: "they are part of a general clause regarding protection and tutelage, as well as the

2. Data Protection and the Pandemic

Many policy determinations are being adopted to face the threat of COVID-19. This includes using technology to assist with contact tracing and social distancing, tools to enable widespread sharing of medical information to accelerate research and creating a digital monetary incentive that would allow individuals to receive immediate financial relief. In this sense, one can cite the Emergency Financial Aid that was already paid in 2020 and that, in 2021/ 2022, workers who registered through Caixa's digital means and members of *Cadastro Único do Governo Federal* (the Single Registry of Federal Government) can check if they are entitled to receive the benefit on the website: www.cidadania.gov.br/auxilio.

The Federal Government's Transparency Portal (General Controllership of the Union) makes the data available in the Detailed Panel of Benefits to Citizens, enabling extensive research, both by citizens in general and by private companies, which can and has already led to the use of the information contained therein for purposes not pursued within the scope of the principles of publicity and transparency, which are duties of the public administration.[14]

Even countries traditionally known for preserving citizens' freedoms, such as the United States, are considering leveraging the technology for the greater good, despite the reduction in personal privacy that will last long after the virus's lifespan. When it comes to COVID-19 detection apps in South Korea and Russia, users' location is not the only thing being tracked. In previous versions of the Russian app, the user's geolocation and camera access permissions, master settings, and address books were requested, and the app regularly transmitted the user's data unencrypted. When combined with Russia's street cameras and the collection of purchase histories, personal privacy is almost non-existent[15]. As

promotion of the human person or a general system of protection for the human person". BIONI, Bruno Ricardo. **Proteção de Dados Pessoais e os limites do consentimento**. p 51.

[14] Let us consider the case of Banco Itaú, which laid off 50 employees using data obtained from the Federal Government's Transparency Portal. Available at: https://exame.com/negocios/itau-demite-50-funcionarios-que-solicitaram-auxilio-emergencial/. Accessed on May 14, 2021.

[15] Coronavirus: Russia's tracking app sparks fury after mistakenly fining users. **EURONEWS**, June 2, 2020. Available at: https://www.euronews.com/2020/06/02/coronavirus-russia-s-tracking-app-sparks-fury-after-mistakenly-fining-users. Accessed on May 12, 2021. Mainly, by Global

for the South Korean app, although the names were erased, individuals often still had enough information to deduce the identity of others. Both measures not only ensure that identities are clear enough for authorities to track, but also allow them to monitor the movements and interactions of individuals long after they have recovered from the virus[16].

As governments plunge into these deep and troubling waters, it is important to realize that there is no turning back. Individual surveillance can and will easily lead to tracking other personal movements and even financial transactions beyond basic browser data or location information. With the issuance of incentives and monetary aid, privacy around online financial transactions is also at stake.

A clear example of this imminent danger can be seen in the present with China's social credit system, as it offers a perfect and modern vision of a very bleak future. For example, if your social credit score is too low, your access to public services will be removed, travel permissions will be denied, and your internet usage will be heavily monitored. The ability of you and your family to attend decent schools or apply for good jobs will be restricted, and the government has the right to publicly shame you on a blacklist[17].

Even medical information is under siege for sharing patient data. While data sharing may seem relatively harmless as far as medicine is concerned, not all data follows patient protection guidelines. When privacy breaches are combined with individual tracking data, purchase data, browser histories and

---

Voice, "*Pandemic Big Brother"*: Highlighting impact of COVID-19 restrictions on digital freedoms in Eastern Europe. **Globalvoices,** March 7, 2021. Available at: https://globalvoices.org/2021/03/07/pandemic-big-brother-highlighting-impact-of-pandemic-surveillance-on-digital-freedoms-in-eastern-europe/. Accessed on May 12, 2021.

[16] About South Korea's successful experience: SCOTT, Dylan. PARKARK, Jun Michael. South Korea's Covid-19 success story started with failure - The inside account of how one country built a system to defeat the pandemic. **VOX,** South Korea. April 19, 2021. Available at https://www.vox.com/22380161/south-korea-covid-19-coronavirus-pandemic-contact-tracing-testing. Accessed on: May 12, 2021.

[17] SUN, Quian. China's social credit system was due by 2020 but is far from ready. **Algorithm Watch,** January 12, 2021. Available at: https://algorithmwatch.org/en/chinas-social-credit-system-overdue/. Accessed on: May 12, 2021. Also the important research report: BACHLSKA, Alicia. China's social credit system and its development: between "Orwellian nightmare" and technocratic utopia? **Asia Research Center Report**, September 2020. Available at: https: //www.academia.edu/44213805/Asia_Research_Centre_Report_September_2020_Chinas_social_credit_system_and_its_development_between_Orwellian_nightmare_and_technocratic_utopia. Accessed on: May 12, 2021.

interactions across communication platforms, companies and governments can build perfect profiles of each person. While technology instigates many of the above problems, it can still help protect privacy in many ways. Zero-knowledge proofs, multiparty computing and homomorphic encryption[18] are just three ways data can be processed and aggregated without revealing the individual details.

Google and Apple have made available a system that employs short-range Bluetooth communications to alert people when they are near an individual diagnosed with COVID-19. While the system currently requires an app and shares some data – which still violates privacy – user consent is required before information is shared, GPS locations are not tracked and any information is transmitted anonymously via keys that circulate regularly[19].

As governments in many countries persist in establishing new methods to track and collect information from individuals, it becomes necessary to continue to develop methods to keep intrusion under control and to continue a step forward in terms of protecting information. Besides that, it is imperative to inquire whether the compensations are proportional to the benefits and whether the authorities can or will be held responsible for any damages or injuries they may cause. Unfortunately, this proportionality does not exist today and, as Edward Snowden stated in an interview, "(...) what is being built is the architecture of oppression[20]."

While the future around personal data may look bleak, there is still time to demand privacy. Everyone must be held accountable for the protection of privacy, which is truly a fundamental human right. As the saying goes: 'privacy loves company'. The more we take responsibility for our own privacy and question the motives of those who wish to suppress our most basic freedom, the greater

[18] The main objective of this type of encryption is to be able to perform operations directly on the encrypted data, without the need to previously decrypt it or to have the key with which it was encrypted, this implies much tighter control over the availability of the information, guaranteeing its integrity and confidentiality. According to: KUNDRO, Daniel. Criptografia homomórfica: um esquema de criptografia cada vez mais usado. **We live security,** September 6, 2019. Available at: https://www.welivesecurity.com/br/2019/09/06/criptografia-homomorfica-um-esquema-de-criptografia-cada-vez-mais-usado/. Accessed on: May 13, 2021.

[19] According to: https: // www.google.com/ covid19/ exposurenotifications/. Accessed on May 14, 2021.

[20] According to Edward Snowden interview for Vice Magazine: Warns Governments Are Using Coronavirus to Build 'the Architecture of Oppression'. **VICE News,** April 9, 2020. Available at: https://www.vice.com/en/article/bvge5q/snowden-warns-governments-are-using-coronavirus-to-build-the-architecture-of-oppression. Accessed on May 12, 2021.

the chance that privacy will once again become the norm rather than the exception is likely. The implications of our decisions now will continue for generations. What's at stake during strange times (?).

During this period of restrictions on people's movement and necessary processing of personal and, in particular, sensitive data (a special category), two diametrically opposed views on the management of the rights crisis have almost automatically emerged. The first considers it inconceivable to discuss the protection of personal data and privacy in such situations and insists that, in the context of dealing with the Pandemic, even the heaviest measures must be taken, introducing methods of real geolocation of the general population and identifiable data processing, not only to those who are sick, but also to their extended family and social circle. The second view, following the same absolutism in the logic of the stratification of arguments, considers that any form of restriction of general protection and restrictions on personal data processing is inconceivable, since it will essentially lead to a new state of interference by the subjects. This will lead to a society under constant supervision (surveillance society).[21]

The design, development and use of digital technologies have ethical and legal implications that cannot be ignored. Digital technologies can indeed improve our quality of life, in particular by making it safer and faster to move out of the current state of restriction, improve public health threats, increase accountability and create new opportunities in many key areas: life in terms of health. On the other hand, they can turn against us if they invade our privacy and limit our ability to participate in society.

This risk has already been perceived in many European countries as we have already reported, for example in Russia where the government has resorted to the use of facial recognition cameras to enforce quarantine measures without sufficient guarantees that this intrusive technology will not be generalized for other purposes[22].

[21] According to this newspaper article: Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco a sua privavidade? **BBC News Brasil,** April 21, 2020. Available at: https://www.bbc.com/portuguese/brasil-52357879. Accessed on May 24, 2021.

[22] According to the **Charter of Fundamental Rights of the European Union**. Available at: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. And according to the **European Convention on**

While digital technologies can help fight the Pandemic, it must not be accepted that they can solve all problems. These should only be used with respect for democratic rules. If governments do not respect these legal limits, they jeopardize our human rights system, without necessarily improving the protection of our health. They also risk losing the trust and support of citizens, a necessary element in the state's efforts to protect human life and health. In this context, it was encouraging that the Committee of Ministers of the Council of Europe, in which all 47 Member States are represented, adopted statements recalling that measures to combat the disease and its wider consequences must be taken in accordance with the Agency's principles and Member States' commitments. This is an important commitment that Member States must fulfill[23].

In fact, in a democracy, respect for privacy should not be sacrificed due to health protection. On the contrary, health and data protection are essential elements for a life with dignity and security. Governments can and must strike the right balance between these two imperative needs and ensure that technology is used to their benefit rather than to the detriment of human rights, democracy and the rule of law.

In order to do this, however, they must follow a series of steps, including the following: (i) first, governments must ensure that digital devices are designed and used in accordance with privacy and equal treatment rules. These devices must be anonymous, encrypted, decentralized, open source and available to as many people as possible, thus eliminating the digital divide that still exists across the planet. Its use must be voluntary, based on informed consent, limited to health

Human Rights. Available at: https: //www.echr.coe.int / Documents/ Convention_POR .pdf. Accessed on May 14, 2021.

[23] According to the Guidelines 4/2020 on the use of location data and means of contact tracing in the context of the COVID-19 outbreak (adopted on April 21, 2020). **European Data Protection Board.** Available in Portuguese at: https: // edpb. europa.eu / sites / default / files / files /file1 /edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Accessed on May 13, 2021. Also, the statement on the data protection impact of the interoperability of contact tracing applications (adopted on June 16, 2020). **European Data Protection Board** Available in Portuguese at: https: // edpb. europa.eu / sites / default / files / files / file1 / edpb_statementinteroperabilitycontacttracingapps _ pt. pdf. Accessed on May 13, 2021. And the Declaration on the processing of personal data in the context of the reopening of borders after the outbreak of COVID-19 (adopted on June 16, 2020). **European Data Protection Board** Available in Portuguese at: https: // edpb. europa.eu / sites / default /files /files /file1 /edpb_statementreopeningbordersanddataprotection_ pt. pdf. Accessed on May 13, 2021.

protection purposes, include a clear time limit and be fully transparent. Users must be able to disconnect at any time, deleting all their data, as well as to report violations of their privacy, resorting to independent and effective solutions. (ii) second, laws that allow states to collect, use and store personal data must strictly comply with the right to privacy, as protected by national and international case law. (iii) third, government actions must be subject to independent scrutiny.

In times when health fears justifiably increase the degree of public acceptance of intervention measures, the need for strong supervision by competent and independent bodies that can operate outside of an emergency case becomes increasingly urgent.

3. Compatibility among LGPD and LAI and LGD: disclosure of personal data on the transparency portal – consent and legitimate interest

Prior to the specific topic of this item, it is important and mandatory to point out that the fundamental right to personal data protection is not an absolute right, in fact, no right has this characteristic, besides, as the pacified doctrine states, personal information is not only an individual's property, since it "integrates the orbit of his representation in the social body, which demands choices made in law or in the Constitution, which demand its processing or its exposure"[24].

In this sense, the article is aimed at analyzing the legality of the disclosure (processing) of personal data and information, on the Federal Government's Transparency Portal, regarding citizens who received the Emergency Financial Aid due to the Pandemic. Initially, to clarify the issue, the CF (the federal constitution) starts with, in a systematic interpretation with the LGPD, LAI and

[24] MENDES, Laura Schertel. RODRIGUES JUNIOR, Otávio Luiz. FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: Rumo a Um Direito Fundamental Autônomo. In: MENDES Laura S., DONEDA, Danilo, SARLET, Ingo W. RODRIGUES JR.., Otávio Luiz (Org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense. 2021. p. 69.

LGD[25], to demonstrate whether or not the disclosure made by the Public Power infringed the right to personal data protection.

The CF, among the principles foreseen as vectors for the Public Administration, foresees, in its article 37, *caput*[26], among others, the principle of publicity. This commandment has its origin and support in the fundamental duty of the State to give broad and general communication of administrative acts, a fact that reveals another right of citizenship, which is free access to information that concerns and interest, in addition to explaining in a republican way a fundamental duty of the State of transparency in all of its administrative actions.

It must be taken into consideration the fact that the republican principle imposes on the public administration and its agents the obligation to act in the promotion and defense of the rights and interests of the community. Moreover, the principle of publicity also imposes the prohibition of secret practices, as well as the exercise of secret acts, except when it comes to matters classified as state security. For that reason, the dissemination/publicity of 'administrative acts' establishes an important management path aimed at expressing the will of the Public Administration, publicizing its content and substance for public knowledge, validating the content of the act in order to promote the production of effects of the administrative act, as well as its legality control.

This principle, it should be noted, is based on the Democratic State of Law in order to promote the participation of society in the control of the acts performed by the Public Administration. As Carvalho Filho points out, this principle is materialized, for example, in the right of petition, the certificates that register the truth of administrative facts, since publicity authorizes the defense or clarification of situations and ex officio administrative action for publicizing information of public interest[27].

---

[25] BRAZIL. **Law nº 14.129 of March 29, 2021** – wich known as the Digital Government Law (LGD). Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on May 12, 2021.

[26] BRAZIL. **Federal Constitucional.** Article 3, *caput.* http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on: April 21, 2021.

[27] CARVALHO FILHO, José do Santos. **Manual de Direito Administrativo.** São Paulo: Grupo Gen. 2018. p. 27.

As it has been said before, the principle of publicity is fundamental in democracies, BOBBIO, perceived that publicity reveals itself as an 'enlightenment category' and represents one of the aspects of the battle of those who consider themselves called to defeat the 'kingdom of darkness'. Therefore, the metaphor of light, of enlightenment, was used to contrast the 'visible power of the invisible'. Thus, giving visibility is to enable access and control of public acts both by society and by the control agencies of each democracy[28].

These days, the principle is even more important. All those involved in the administration, whether they are public or supervisory authorities and courts, gradually found themselves and are faced with the challenge of giving life to normative texts in a classical environment that essentially relies on “paper”. However, in today's reality, that of an increasingly electronic context, everything changes. Computers invaded every floor of the administrative areas. Networks connect machines and men systematically, allowing dialogue and exchanges far beyond the initially compartmentalized departments. Electronic servers are open at any time of day, ready to provide requested information and receive completed forms. The entire administration became electronic, and now we are talking about Electronic Government or Digital Government (DG).

The benefits of technological advances are not without raising questions and highlighting difficulties. Furthermore, the identification of the person with information in an electronic administration or e-government context is not obvious, due to the shift from 'compartment' administration to 'network administration'. However, for this principle to be met, it is not enough to publicize the acts, the principle of publicity has a qualification derived from another principle, that of transparency.

With the advent of ICTs, the possibility of making the acts of the administration public, at the highest possible level, increased transparency and gave strength to the democratic aspect by establishing a channel via a global network of direct communication between citizens and the Public Power. This sort of new means of communication resulted in a deepening of democracy and in greater publicity, transparency and efficiency in public activity, as it was more

[28] BOBBIO, Norberto. **O futuro da democracia**. 7ª ed. São Paulo: Paz e Terra, 2000, p. 103.

controlled through the constitutional mechanisms made available to society. Information pluralism, free access and circulation of information act as a general rule to provide control. However, as mentioned above, what is “publicized” on the world wide Web does not always translates into transparency.

Although the Federal Constitution did not anticipate the ‘principle of transparency’, expressly, in the list of principles that regulate public administration contained in the caput of article 37, it can be extracted from the combination of the principle of publicity with the right to information (art. 5, XXXIII) in conjunction with the democratic principle. For that reason, publicity aims, through clear and objective disclosure, to ensure that the act was performed in accordance with legality, morality and other constitutional precepts, whereas transparency is what Freitas calls “noon sun visibility”.[29] It is not enough to make known what is done, but to do it in a way that everyone understands without difficulties or obscure paths in the information portals or elaborate language that hinders the objective of bringing the acts of the administration to light.

The principles of transparency and publicity are fundamental for the accomplishment of the right of access to public information[30]. Transparency is an essential prerequisite for the credibility and integrity of public institutions in order to promote public trust and support. Transparency in public administration ensures legal certainty and increases the level of legitimacy in decision-making processes. In addition to that, the principle of transparency guards a concentrated impulse of the 'administration's responsibility towards citizenship', ensuring and allowing this possession to reach all information about the affairs of the public administration and, in the same way, to be able to commit itself in the processes of decision-making.

Transparency in public administration has a major impact on the public administration reform process and promotes the level of efficiency, effectiveness and responsiveness as key components of the concept of good administration.

[29] FREITAS, Juarez. **O Controle dos Atos Administrativos e os Princípios Fundamentais**. São Paulo: Malheiros Editores, 2013, p.77.
[30] For a deeper understanding of: BALL, Carolyn. What Is Transparency? **Public Integrity**, vol. 11, 4ªed., p. 293–308, 2009. Available at (*pay-per-view)*: https://www.tandfonline.com/doi/abs/10.2753/PIN1099-9922110400. Accessed on May 15, 2021.

In Brazil, the Transparency Law (LT), Complementary Law nº 131/2009, amended the wording of the Fiscal Responsibility Law (LRF), Complementary Law 101/2000, reinforcing the fact that LRF defends transparency in fiscal management. Two years later, the Access to Information Law was enacted (Law nº 12.527/2011), thus, added to the LRF and LF, they all work so that citizens have broad access and transparency in the information provided by the Government.

Two models of transparency and accessibility to Information of public importance are recognized. The first is what is offered as 'proactive transparency', this model involves the publication of information of public importance before the collectivity or the citizen requests it. In Brazil, it is the Transparency Law (LT) which orders agencies to be ' proactive' in terms of disseminating information. Essentially, this hypothesis is the belief that all information of public importance concerns the public, and that it is only in the possession of Government agencies[31]. The second model, presented as 'reactive transparency'[32], in Brazil is the Access to Information Law (LAI) which ensures that whoever requests the information will receive it. It is also about the public's right to know, but in this case it is done at popular demand.

Transparency in public administration at the same time implies the promotion and access to public information, which may consist of different policy data and memories, but also cartographic information, meteorological data, registration data, actions, investments, application of resources for society and for administration entities, budget and management data, and so on. Through digitization, public information has become a topic of imperative interest, mainly as raw material for a knowledge-based economy. Transparency and privacy are not antonyms, but there are clear tradeoffs between them. This has to do with the

[31] DARBISHIRE, Helen. Proactive Transparency: The future of the right to information? A review of standards, challenges, and opportunities. **The World Bank,** September 14, 2010. Available at: http:// documents.worldbank.org/curated/en/100521468339595607/Proactive-transparency-the-future-of-the-right-to-information-A-review-of-standards-challenges-and-opportunities. Accessed on May 15, 2021.

[32] FAINI, Fernanda; PALMIRANI, Monica. The Right to Know and Digital Technology: Proactive and Reactive Transparency in the Italian Legal System: **7th International Conference EGOVIS**, Regensburg, Germany, September 3–5, 2018. Available at (pay-per-view): https://link.springer.com/chapter/10.1007/978-3-319-98349-3_13. Accessed on May 15, 2021.

public administration, which manages large amounts of citizens' personal data. Interestingly enough, to hold the public administration accountable for the use of this information, transparency[33] is often required. Finally, public administration transparency has repercussions on global indicators of good governance and economic performance, which are also increasingly measured by such comparative assessments[34].

In fact, as an indication of good governance, transparency is exclusively dedicated from the economic and financial point of view, by the way, see in Brazilian law, the imperatives embodied in Complementary Law nº 101/2000, Fiscal Responsibility Law and Complementary Law nº 131/2009, Transparency Law. In them, we can find the commandment that points out that 'responsibility in fiscal management presupposes planned and transparent action', as follows: ‘they are instruments of transparency of fiscal management, which will be given wide dissemination, including in electronic means of public access: the plans, budgets and budget guideline laws; the rendering of accounts and the respective prior opinion; the Budget Execution Summary Report and the Fiscal Management Report; and the simplified versions of these documents.

Also, Law nº 14.129 of 03/29/2021 (with deferred validity for different moments of its publication)[35], wich called the Digital Government Law (LGD) provides for principles, rules and instruments for Digital Government (DG, also e-Gov). It points out ways to improve the efficiency of public administration through the digitization of records and the use of technology to make public services, agencies and development more franchisable and accessible to the population, covering low-income strata or residents in rural and isolated areas[36]. Established in 2016, the Digital Government essentially intends for the State to approach its citizens more effectively, to provide more efficient and higher quality services,

[33] For a deeper understanding of: DE ARRUDA, Carmen Silvia L. O. **Princípio da Transparência.** São Paulo: Editora Quartier Latin; 1ª ed, 2019.
[34] On this subject the very well organized **Worldwide Governance Indicators Project** (WGI) of the World Bank. Available at: https://info.worldbank.org/governance/wgi/. Accessed on May 18, 2021.
[35] BRAZIL, **Law nº 14.129 of March 29, 2021**, Article 55. Available at: http: //www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on May 12, 2021.
[36] BRAZIL, **Law nº 14.129 of March 29, 2021**, Article 55. Available at: http: //www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on May 12, 2021.

agency and promotion, as well as to reduce the need for personal contact with public agents.

With the publication of Decree nº 8.638, of 02/15/2016, the Digital Governance Policy was created for the bodies and entities of the direct, autonomous and foundational federal public administration, with the purpose of boosting employment, by the public sector, of information and communication technologies (ICT) in order to improve information and the provision of services, agency and promotion. All that with the purpose of stimulating the participation of citizens in the decision-making process and making the government more responsible, transparent and effective[37], tracing a roadmap for the digitization of public services. Initiatives such as the publication of a performance dashboard (updated weekly and found on the Services Dashboard (servicos.gov.br) allow citizens to track the progress of digitization made to date and reflect the government's often stated desire for transparency.

As per Decree nº 10.332 of 04/29/2020, Decree nº 8.638, of 02/15/2016 was revoked, and the Digital Government Strategy for the period from 2020 to 2022 was instituted, within the scope of the bodies and entities of the direct federal, autarchic and foundational public administration[38]. Otherwise, and connected to the DG where relevant, the LGD is applicable to the federal government and its various administrations, public companies and government-controlled companies (including its subsidiaries and controlled companies). It must be implemented in line with Brazilian data protection legislation, the LGPD (similar to the European GDPR[39]).

Still in the same scenario as the DG and formally prior to it, in the Brazilian legal system, the exercise of the right to information is enshrined in Law nº. 12.527/11[40] – Law on Access to Information (LAI). It is a procedural law that

---

[37] Digital government Strategy for the 2020 period. **Gov.br,** November 25, 2019. Available at: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/historico. Accessed on May 13, 2021.

[38] BRAZIL. **Decree nº 10.332 of April 28, 2020**. Available at: http://www.planalto.gov.br/ccivil_03/ato2019-2022/2020/decreto/D10332.htm. Accessed on May 17, 2021.

[39] GENERAL DATA PROTECTION (GDPR). **GDPR.info.** Available at: https://gdpr-info.eu. Accessed on May 17, 2021.

[40] BRAZIL. **Law nº 12.527, of November 18, 2011**. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on April 21, 2021.

incorporates the basic principles of the CF and establishes guidelines and ensures that public entities must disclose at least a list of “minimum” information that is of public or collective interest. Some aspects contained in the LAI initially lead those who learn about it to ask: if the acts of the administration, according to the CF and LAI, must be public and access to information is a fundamental right, what is the basis for disclosing personal data, where secrecy is the norm? In order to be able to answer this question, it is necessary to score according to the guidelines contained in article 3 of the standard[41]. Here, in advance, we can already see the importance of the 'principle of publicity', that is, publicity is the rule (general precept) and secrecy is the exception.

Until recently, the systematic use of personal data was basically carried out by the State, which, given the high cost of technology, was the only entity capable of collecting (through censuses and surveys) and managing the information[42]. The LGPD that regulates “informational privacy” and provides for the processing of personal data applies to natural persons and legal entities governed by public or private law and among its various foundations are respect for privacy and informational self-determination. The protection of personal data, by LAI, has reached a peculiarly protected normative framework, as an 'exception to transparency' typical of democracies. There, the definition of "personal information" was articulated in the same content demarcated today by the LGPD, personal data, those related to the identified or identifiable natural person[43].

According to LAI’s normative command, the Public Power is awarded the protection of personal information, “subject to its availability, authenticity, integrity and possible access restriction[44]”. It should be noted that the scope of protection (personal) ensures access reserved for previously qualified public agents and, of

[41] BRAZIL. **Law nº 12.527, of November 18, 2011**, Article 3. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on April 21, 2021.
[42] RUARO, Regina Linden; REIS, Fernando Simões dos. A anonimização dos dados como forma de relativização da proteção de informações sigilosas e a atuação fiscalizadora dos Tribunais de Contas. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor.** Brasília, v.5, nº2, p.157-187, july-december, 2018. Available at: https://portalrevistas.ucb.br/index.php/REPATS/article/view/9393. Accessed on May 14, 2021.
[43] BRAZIL. **Law nº 12.527, for November 18, 2011**. Article 4. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on April 21, 2021.
[44] BRAZIL. **Law nº 12.527, for November 18, 2011**. Article 6. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on April 21, 2021.

course, those individuals to whom the information concerns, regardless of their classification (level of secrecy), guaranteeing access to third parties, provided that by court decision or express permission of the data subjects[45]. The waiver of consent can be given in cases of health care, sanitary measures, incapacity of the holder and for research methodology and scientific procedure, all situations that meet the public interest, provided that the identity of the holder and other restrictions are protected[46].

More recently, in addition to being understood in the field of DG, we have the LGPD, applied to the public and private domains, establishing a balance between data protection and promoting the privacy of citizens, and in the public sector, the use of these data for the elaboration and execution of public policies, as well as the appropriate provision of public services. Three types of data with different levels of protection are regulated by the LGPD: (a) personal data, (b) sensitive personal data, and (c) anonymized data. Personal data reveals any information relating to an identified or identifiable person. Sensitive personal data means personal data "about racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data" of a particular person.

Finally, anonymized data is the result of a treatment procedure that ensures that the data of holders remain anonymous, the requirements of the law no longer apply to them. This makes it possible for them to be shared in databases that are properly anonymized, provided, of course, that the anonymization procedure is fully reliable and irreversible[47]. LAI, LGDP and LGO as a framework of Digital Government, indispensable for a quality Administration, are normative instruments that are at the base of support of affirmative or

[45] BRAZIL. **Law nº 12.527, for November 18, 2011**. Article 31. Available at: http: //www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on April 21, 2021.
[46] BRAZIL. **Law nº 12.527, for November 18, 2011**. Article 31, Paragraph 3. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on April 21, 2021.
[47] BRAZIL. **Law nº 13.709, for August 14, 2018**. Article 5. Available at: http://www. planalto.gov.br / ccivil_03 /_Ato2015-2018 / 2018 / Lei / L13709.htm. Accessed on April 21, 2021.

negative theses of the legitimacy of the disclosure of data of those who received emergency financial aid as a result of the COVID-19 crisis.

The LGPD provides the conditions to situate the 'legal bases for the processing of personal data', including the 'need for consent of the subject' and, in the absence of such consent, among others, the 'legitimate interest', establishing requirements so that data processing can be carried out. The main requirement is that the data subject gives explicit consent to the treatment, in writing or unequivocally, with a specific and pre-defined purpose. However, although the existence of consent from the holder regarding personal data is a basic requirement that enables data processing, it is not the only one and does not have the power to hinder data processing in its absence. The Law admits the processing/operation of personal data even when the data subject's consent is not available, provided that, it is observed, this condition proves to be indispensable for the Administration to promote and satisfy public policies, or for research bodies to be able to produce research and studies or so that the controller, among other circumstances, meets 'its legitimate interests or those of a third party', unless the fundamental rights of the holder that demand the protection of personal data must prevail.

The 'legitimate interest' is the assumption of greater flexibility in terms of 'legal authorization' for the processing/operationalization of personal data. On the other hand, it should not and cannot be used as an asset to validate the data base and waive the consent from the data subjects. In this sense, the LGPD adds certain precautions that need to be taken when performing the treatment/operationalization based on this foundation. Note that if it is based on legitimate interest, only personal data that is strictly essential for the desired purpose may be processed. Moreover, the controller will need to take appropriate actions and measures in order to ensure the 'transparency of' the treatment/operationalization of data based on its 'legitimate interest'.

In the case of disclosure of data on beneficiaries of the Government's economic-financial assistance programs who had their data exposed on the Federal Government's Transparency Portal, part of the doctrine leans towards

the violation by the Government of the privacy of the beneficiaries[48]. This position, as it seems, points to becoming a majority based one, says that “after consulting the links of the lists published by the federal government, it is possible to verify that among the information disclosed are the state, the city, the social identification number (NIS), the CPF – Individual Taxpayer ID No. (six middle digits), the full name of the beneficiary and the amount received from the emergency financial aid by each citizen[49]”. In spite of the very well articulated reasons of those authors who argue that the disclosure of this data hurts the LGPD and implies the Public Power in the responsibility for the violation of the data, regarding these reflections - except for our intellectual misunderstanding - we think otherwise.

First, we take into account the 'big picture' in which the planet finds itself. The unprecedented situations we have been experiencing in recent times (at least from the last quarter of 2019 to the present) have truly put us to the test. For the first time in many decades, people, especially in the Western world, are facing a terrible threat that jeopardizes not only prosperity and everyday life, but our very existence. At the same time, we are dealing, quite painfully, with the realization of legal concepts that younger generations have never experienced to such an extent as cases of force majeure, and breach of our individual rights in the public interest. These conditions mark a moment for the Administration, which on the one hand has to firmly assume the control of managing a major crisis that threatens to disrupt social cohesion, public health and the stability of the State. On the other hand, it will be put to the test by limiting, to a significant degree, basic individual rights. The conflict of these rights seems inevitable.

The right to the protection of our data is not an absolute right, as stated above, it is defined from the beginning by the constitutional and legal statute itself. This must also be evaluated in relation to its role in society and weighed against

[48] By all, according to OLIVEIRA, Adriana Carla Silva de; ARAÚJO, Douglas da Silva. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **LIINC em Revista**. Rio de Janeiro, v. 16, nº 2, December, 2020. Available at: https://doi.org/10.18617/liinc.v16i2.5318. Accessed on May 19, 2021.

[49] OLIVEIRA, Adriana. **O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados**. Available at: https://doi.org/10.18617/liinc.v16i2.5318. Accessed on May 19, 2021.

other fundamental rights, in accordance with the principle of proportionality. The right to information may also be limited. Whether as freedom of expression and freedom of the press or as the right to know what is happening, this disclosure may have to be tolerated regarding both the non-disclosure of certain data and its disclosure in order to control a Pandemic crisis. Also in this case, the criterion cannot be the “thirst” of the public for information that affects privacy without value for the public interest. The public's reasonable interest is limited by the need to protect information that is not discloseable, so it is extremely interesting to measure proportionality in these cases. Just as important is the effort to limit the circulation of false and non-existent rumors that can cause significant damage to both the public and individual interest. At the same time, waves of “outraged” citizens are generated against those responsible for managing the crisis and with governments proposing restrictive measures.

Final Considerations

During this period of restrictions on people’s movement and necessary processing of personal and, in particular, sensitive data, two diametrically opposed views on the management of the rights crisis have almost automatically emerged. The first considers it inconceivable to discuss the protection of personal data and privacy in such situations, in the context of dealing with the Pandemic, even the heaviest measures must be taken, notably with regard to public resources. The reflection, following the same absolutism in the logic of the stratification of arguments, will be to consider that any form of mitigation of general protection and restrictions on the processing of personal data is inconceivable, since it will essentially lead to a new state of supervision of individuals, this will lead to a society of constant surveillance.

It is not the purpose of this study, for its brevity and for not intending to end discussions on the matter, it should be emphasized, however, that historically the greatest reward for the use of interventions (and mainly through new technologies) that enter the sanctuaries of our personal life is the satisfaction of

the feeling that seems to be most threatened: the feeling of security and protection (provided by the State). So much so that individuals in “dangerous” circumstances make the greatest concessions to preserve personal, family and work safety and do not focus, at the heart of privacy.

Notwithstanding this, the study can demonstrate that it is necessary to balance the social benefit (such as economic aid benefits) with the state restriction of individual rights, developing balance tests, so that the specific conditions under which it is necessary to restrict an individual right can be outlined. Still within the scope regarding the terminology of personal data, it seems, nevertheless, that before the application of administrative measures, which restrict individual rights, we need human rights impact assessments and a national accountability system. The greatest justification for disclosing beneficiary data – in these modest reflections – is primarily based on the Principle of Transparency, because as we previously stated, transparency in Public Administration ensures legal certainty and expands the level of legitimacy in decision-making processes, and herein the decision involves the binary scope of economic, State and Citizenship protection.

Furthermore, the principle of transparency guards a concentrated impulse of the 'administration's responsibility towards the citizen', ensuring and allowing that it can reach all the information about the affairs of the public administration and, in the same way, can be involved in the processes of decision-making, to commit to the resources made available to them, notably because they form a stratum of the population that benefits from their own vulnerability. As a second foundation, the LAI and LGPD ensure the disclosure by the Public Power given the existence of a legitimate interest for the processing/operationalization of data, besides, this is essential to achieve this legitimate interest. It should be noted that in this case there is no other legal basis to be exercised, as it is not possible to obtain prior consent, for this reason the Transparency Portal and DATAPREV used the data for a single (specific) purpose and only the necessary data, keeping that same data with integrity.

Otherwise, a (fictitious) consent of the beneficiaries can also be assumed for the acceptance and receipt of the same benefit, however, this presumption is

not necessary. Note that the Transparency Portal categorizes data by Region, State, Municipality and Beneficiary Name, as well as the root of your CPF (Individual Taxpayer Registration No.), that is, only the six central numbers of the document, the social identification number (NIS) only appears in in some cases, even the amount received, as it can be concluded, the beneficiary's right is protected and even the LGPD points out the following: right to have the processing of data limited to what is strictly necessary for the intended purpose when the processing is based on the legitimate interest of the controller (Art. 10, Paragraph 1), likewise ensured the right to transparency in data processing based on the controller's legitimate interest (Art. 10, Paragraph 2, our emphasis). Finally, note that, not yet provided for in the LGPD, as it was in the European GDPR, opportunistic disclosure passes the proportionality test.

The proportionality test is intended to weigh the feasibility of using the legal basis of legitimate interest. The aim is to balance, on the one hand, the interests of the Public Power, on the other, the rights of the holder of personal data. Three vectors can be pointed out: legitimacy of interest, necessity, consideration (or rationality). The LGPD, in its article 10, states that it assists the controller with the grounds for the processing/handling of personal data for the proper development of its activities, legal rights and duties. As for legitimacy, the very magnitude of the aid program attests to its presence; as for the need, the Public Power only used the minimum data necessary to identify the beneficiaries and, thus, provide security in the provision of resources; regarding the weighting (rationality) deriving from the presence of the legitimate interest; it was not exercised in an invasive or discriminatory way, the procedure having met the expectations of the provider of transparency and smoothness of the operation and, mainly, meeting the fundamental rights of the beneficiaries, preserving their privacy as much as possible.

Finally, it is also worth arguing that disclosure guarantees the integrity of the assistance program, including delimiting the population stratum affected and preventing fraud (which, nevertheless, occurred accordingly). Certainly, when we receive public funds, publicity and transparency are requirements of the very democratic structure of social assistance programs. They are, moreover,

requirements of a legitimate republicanism committed to good faith, with clarity and social responsibility.

References

BACHLSKA, Alicia. China's social credit system and its development: between “Orwellian nightmare” and technocratic utopia? **Asia Research Center Report**, setembro, 2020. Available at: https: // www.academia.edu / 44213805/ Asia_Research_Centre_Report_September_2020_Chinas_social_credit_system_and_its_development_between_Orwellian_nightmare_and_technocratic_utopia. Accessed on May 12, 2021.

BALL, Carolyn. What Is Transparency? **Public Integrity**, vol. 11, 4ªed., p. 293–308, 2009. Available (*pay-per-view)* at: https://www.tandfonline.com /doi /pdf/10.2753/PIN1099-9922110400?needAccess=true. Accessed on May 15, 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais e os limites do consentimento.** Rio de Janeiro: Editora Forense. 2020.

BOBBIO, Norberto. **O futuro da democracia**. 7ª ed. São Paulo: Paz e Terra, 2000.

BRAZIL. **Complementary Law nº 101 of May 4, 2000.** Establishes norms of public finances focused on responsibility in fiscal management and other provisions. Available at: http:// www.planalto.gov.br / ccivil_03 / leis/lcp/lcp101.htm. Accessed on: May 12, 2021.

BRAZIL. **Constitution of the Federative Republic of Brazil 1988**. Available at: http: // www.planalto.gov.br / ccivil_03/ constituicao / constituicao.htm. Accessed on: April 21, 2021.

BRAZIL. **Decree nº 592 of July 6, 1992.** Internalizes the International Covenant on Civil and Political Rights, adopted by Resolution 2.200-A (XXI) of the United Nations General Assembly, on December 19, 1966. Available at: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Accessed on: May 12, 2021.

BRAZIL. **Decree nº 9.319 of March 21, 2018**. Institutes the National System for Digital Transformation and establishes the governance structure for the implementation of the Brazilian Strategy for Digital Transformation. Available at: http://www.planalto.gov.br/ccivil_03/Ato2015-2018/2018/ Decreto / D9319. htm. Accessed on: May 17, 2021.

BRAZIL. **Decree nº 9.637 of December 26, 2018.** Establishes the National Information Security Policy, provides for the governance of information security, and amends Decree nº 295, of August 4, 1997, which regulates the provisions of Article 24, caput, item IX, of Law nº 8666, of June 21, 1993, and provides for the waiver of bidding in cases that may compromise national security. Available

at: http://www.planalto. gov.br/ ccivil_03 / Ato2015 – 2018 / 2018 / Decreto / D9637. htm. Accessed on: May 17, 2021.

BRAZIL. **Decree nº 9.756 of April 11, 2019.** Establishes the single portal "gov.br" and provides rules for unifying the federal government's digital channels. Available at: http://www.planalto.gov.br / ccivil_03/_ato2019-2022 / 2019/ decreto / D9756. htm. Accessed on: May 17, 2021.

BRAZIL. **Decree nº 9.854 of June 25, 2019.** Establishes the National Plan for the Internet of Things and provides for the Chamber for Managing and Monitoring the Development of Machine-to-Machine Communication Systems and the Internet of Things. Available at: http:// www.planalto.gov.br/ccivil03/Ato2019-2022/2019/Decreto/D9854.htm. Accessed on: May 17, 2021.

BRAZIL. **Decree nº 10.278 of March 18, 2020**. Regulates the provisions of item X of the caput of art. 3 of Law nº 13.874, of September 20, 2019, and art. 2-A of Law nº 12.682, of July 9, 2012, to establish the technique and requirements for the digitization of public or private documents, so that the digitized documents produce the same legal effects as the original documents. Available at: http: //www. planalto. gov.br / ccivil_03 /_ Ato2019-2022/2020 / Decreto /D10278. htm. Accessed on: May 17, 2021.

BRAZIL. **Decree nº 10.332 of April 28, 2020**. Establishes the Digital Government Strategy for the period from 2020 to 2022, within the scope of organs and entities of the direct federal, autonomous and foundational public administration, and makes other provisions. Available at: http: //www. planalto.gov.br/ ccivil_03 /_ato2019-2022 / 2020 / decreto / D10332. htm. Accessed on: May 17, 2021.

BRAZIL. **Decree nº 10.661 of March 26, 2021.** Regulates Provisional Measure nº 1.039, of March 18, 2021, which institutes the Emergency Aid 2021 for facing the public health emergency of international importance due to the Coronavirus (Covid-19). Available at**:** http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10661.htm Accessed on: May 17, 2021.

BRAZIL. Federal Supreme Court (Plenary). **Referendum in Precautionary Measure in ADI 6.387/DF.** Minister Rosa Weber. May 7, 2020. Available at: http: //redir.stf.jus.br /paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Accessed on: April 20, 2021.

BRAZIL. **Law nº 12.527 of November 18, 2011.** Access to Information Law. Regulates the access to information provided for in item XXXIII of art. 5, in item II of §3 of art. 37 and in §2 of art. 216 of the Federal Constitution; amends Law nº 8112 of December 11, 1990; revokes Law nº. 111 of May 5, 2005, and provisions of Law nº 8159 of January 8, 1991; and makes other provisions.

Available at: http://www.planalto.gov.br/ ccivil_03 /_ato2011- 2014 / 2011 / lei / l12527.htm. Accessed on: May 17, 2021.

BRAZIL. **Law nº 13.709 of August 14, 2018**. General Law for the Protection of Personal Data (LGPD). Available at: http: //www.planalto.gov.br/ ccivil_03/_ato2015-2018 /2018 / lei / l13709 .htm. Accessed on: May 12, 2021.

BRAZIL. **Law nº 13.979 of February 6, 2020**. Provides for measures to address the public health emergency of international importance arising from the coronavirus responsible for the 2019 outbreak. Available at: http: // www.planalto.gov.br / ccivil_03 /_ato2019-2022 / 2020 /lei /l13979.htm. Accessed on: May 12, 2021.

BRAZIL. **Law nº 14.129 of March 29, 2021.** Provides on principles, rules, and instruments for Digital Government and for increasing public efficiency and amends Law nº. 7.116 of August 29, 1983, Law nº 12.527 of November 18, 2011 (Access to Information Law), Law nº. 12.682 of July 9, 2012, and Law nº 13.460 of June 26, 2017. Available at: http: // www.planalto.gov.br / ccivil_03 /_Ato20192022/2021 / Lei/L14129.htm#art55. Accessed on: May 12, 2021.

BRAZIL. **Legislative Decree 6 of 2020.** Recognizes, for the purposes of article 65 of Complementary Law No. 101, of May 4, 2000, the occurrence of a state of public calamity, in accordance with the request of the President of the Republic forwarded through Message nº. 93 of March 18, 2020. Available at: http://www.planalto.gov.br/ccivil_03/portaria/DLG6-2020.htm. Accessed on: May 12, 2021.

BRAZIL. **Lei Complementar nº 131, de 27 de maio de 2009.** Acrescenta dispositivos à Lei Complementar nº 101, de 4 de maio de 2000, que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências, a fim de determinar a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp131.htm. Accessed on: May 12, 2021.

CARVALHO FILHO, José do Santos. **Manual de Direito Administrativo**, São Paulo: Grupo Gen. 2018

CORONAVIRUS: Russia's tracking app sparks fury after mistakenly fining users. **EURONEWS**, 02/06/2020. Available at: https: // www.euronews.com / 2020 /06/02/coronavirus-russia-s-tracking-app-sparks-fury-after-mistakenly fining-users. Accessed on: May 12, 2021.

COUNCIL OF EUROPE. **European Convention on Human Rights**. Available at: https: // www.echr.coe.int / Documents/Convention_POR.pdf. Accessed on: May 14, 2021.

DARBISHIRE, Helen. Proactive Transparency: The future of the right to information? A review of standards, challenges, and opportunities. **The World Bank,** 14/09/2010. Available at: http:// documents. worldbank.org /curated /en /100521468339595607/Proactive-transparency-the-future-of-the – right - to-information- A – review – of - standards- challenges – and - opportunities.

DE ARRUDA, Carmen Silvia L. O. **Princípio da Transparência.** São Paulo: Editora Quartier Latin; 1ª ed, 2019.

DECLARATION ON THE HANDLING OF PERSONAL DATA IN THE CONTEXT OF THE REOPENING OF BORDERS AFTER THE COVID-19 OUTBREAK (adopted June 16, 2020). **European Data Protection Board.** Available at: https: //edpb.europa.eu/sites/default/files/files/file1/edpb_statementreopeningbordersanddataprotection_pt.pdf. Accessed on: May 13, 2021.

DECLARATION OF SANTA CRUZ DE LA SIERRA. Available at: https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf. Accessed on: May 11, 2021.

DECLARATION ON THE IMPACT ON DATA PROTECTION OF THE INTEROPERABILITY OF CONTACT TRACKING APPLICATIONS (adopted June 16, 2020). **European Data Protection Board.** Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpbstatementinteroperabilitycontacttracingapps_pt.pdf. Accessed on: May 13, 2021.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico**.** Joaçaba, v. 12, nº 2, p. 103, july-december, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** São Paulo: Revista dos Tribunais, 2019, p.169.

EUROPEAN COURT OF HUMAN RIGHTS. Guide on Article 8 of the Convention – Right to respect for private and family life. Available at: https://www.echr.coe.int /Documents /Guide _Art_8_ENG . pdf. Accessed on: May 13, 2021.

EUROPEAN PARLIAMENT: **Charter of Fundamental Rights of the European Union.** Available at: https: // www.europarl. europa. eu / charter / pdf / text_pt. pdf. Accessed on: May 14, 2021.

FAINI, Fernanda; PALMIRANI, Monica. The Right to Know and Digital Technology: Proactive and Reactive Transparency in the Italian Legal System: **7th International Conference EGOVIS**, Regensburg, Germany, September 3–

5, 2018. Available (pay-per-view) at: https: //link.springer.com /chapter /10.1007/ 978-3-319-98349-3_13. Accessed on: May 15, 2021.

FINCATO, Denise; GILLET, Sergio Augusto. **A Pesquisa Jurídica sem Mistérios**. Recife: Editora Fi, 2018.

FREITAS, JUAREZ. **O Controle dos Atos Administrativos e os Princípios Fundamentais.** São Paulo: Malheiros Editores. 2013

GLOBAL VOICE. "*Pandemic Big Brother*": Highlighting impact of COVID-19 restrictions on digital freedoms in Eastern Europe. **Globalvoices,** 07/03/2021. Available at: https:// globalvoices.org/2021/03/07/pandemic-big-brother-highlighting - impact-of-pandemic-surveillance-on-digital-freedoms-in-eastern-europe/. Accessed on: May 12, 2021.

GOV.BR. Estratégia de Governo Digital para o período de 2020. **Gov.br,** 25/11/2019. Available at: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/historico. Accessed on: May 13, 2021.

GUIDELINES 4/2020 ON THE USE OF LOCATION DATA AND MEANS OF TRAILING CONTACTS IN THE CONTEXT OF THE COVID-19 SURGE (adopted April 21, 2020). **European Data Protection Board.** Available at: https:// edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Accessed on: May 13, 2021.

KUNDRO, Daniel. Criptografia homomórfica: um esquema de criptografia cada vez mais usado. **We live security,** 06/09/2019. Available at: https: // www.welivesecurity.com/br / 2019/09/06/ criptografia-homomorfica-um-esquema-de-criptografia-cada-vez-mais-usado/. Accessed on: May 13, 2021.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. **Curso de Direito Constitucional.** São Paulo: Revista dos Tribunais, 2014.

MENDES, Laura Schertel. RODRIGUES JUNIOR, Otávio Luiz. FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: Rumo a Um Direito Fundamental Autônomo. In: MENDES Laura S., DONEDA, Danilo, SARLET, Ingo W. RODRIGUES JR.., Otávio Luiz (Org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense. 2021.

OLIVEIRA, Adriana Carla Silva de; ARAÚJO, Douglas da Silva. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **LIINC em Revista**. Rio de Janeiro, v. 16, nº 2, dez.2020. Available at: https://doi.org/10.18617/liinc.v16i2.5318. Accessed on: May 19, 2021.

RUARO, Regina Linden. REIS, Fernando Simões dos. A anonimização dos dados como forma de relativização da proteção de informações sigilosas e a atuação fiscalizadora dos Tribunais de Contas. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor.** Brasília, v.5, nº2, p.157-187, july-december, 2018. Available at: https://portalrevistas.ucb.br/index.php/ REPATS/ article/ view/ 9393. Accessed on: May 14, 2021.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. In: MENDES, Laura., DONEDA, Danilo., SARLET, Ingo. RODRIGUES JR., Otávio. (Org.) **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense. 2021.

SCOTT, Dylan. PARKARK, Jun Michael. South Korea's Covid-19 success story started with failure - The inside account of how one country built a system to defeat the pandemic. **VOX,** Coréia do Sul. 19/04/2021. Available at: https:// www.vox.com /22380161/south-korea-covid-19-coronavirus-pandemic-contact-tracing-testing. Accessed on: May 12, 2021.

SINAL ORG. Sinal Org, 2020-2021. **Tracking, surveillance and privacy.** Available at: https://signal.org/en/. Accessed on: May 14, 2021.

SNOWDEN: WARNS GOVERNMENTS ARE USING CORONAVIRUS TO BUILD 'THE ARCHITECTURE OF OPRESSION'. **VICE News,** 09/04/2020. Available at: https://www.vice.com/en / article / bvge5q/ snowden - warns-governments - are - using – coronavirus – to – build – the – architecture – of - oppression. Accessed on: May 12, 2021.

SUN, Quian. China's social credit system was due by 2020 but is far from ready. **Algorithm Watch,** 12/01/2021. Available at: https: // algorithmwatch.org /en / chinas-social-credit-system-overdue/. Accessed on: May 12, 2021.

VINCENT, David. **Privacy: A Short History**. Cambridge/UK: Polity, 2016.

WARREN, Samuel D.; BRANDEIS, Louis. **The right of privacy**. Harvard Law Review, Dec. 15, 1890, vol. 4, nº 5. Available at: https://www.jstor.org /stable /1321160. Accessed on: May 14, 2021.

WORLD BANK. **Worldwide Governance Indicators (WGI) Project**. Available at: https://info.worldbank.org/governance/wgi/. Accessed on May 18, 2021.