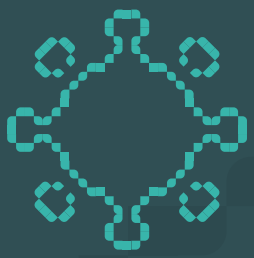
Data
Privacy
Brasil
Research



REPORT

Privacy and pandemic:

Recommendations for the legitimate use of data in the fight against Covid-19

Bruno Bioni | Rafael Zanatta | Renato Leite Monteiro and Mariana Rielli

DataPrivacyBR
Research

Data Privacy Brasil Research

REPORT

Privacy and pandemic

Recommendations for the legitimate use of data in the fight against COVID-19

São Paulo
April 13th 2020

Presentation

Data Privacy Brasil was founded to develop a culture of personal data protection in Brazil. The organization is based in São Paulo, and in less than two years, it has trained more than 2000 professionals from different backgrounds, including professionals from both private and public sector, academics, members of non-governmental organizations, and members of the Public Defender's Office. One of Data Privacy Brasil's goals is to help public officials, regulators, judges, and legal professionals deal with complex questions that require deep knowledge of how socio-technical systems directly affect fundamental rights.

Data Privacy Brasil Research Association, created in 2020 from the school's experience, is focused on socio-legal investigations about the interconnection between personal data protection, technology, and fundamental rights. Through the Observatory on Privacy and Data Protection, the organization constantly monitors regulatory decisions from data protection authorities all around the world, strategic cases on the Brazilian judiciary and international courts, and new bills that can change the regulatory scenario. Furthermore, one of its goals is the production of policy papers and other position documents to help the authorities responsible for decision-making.

Combining research skills and vast experience on the Brazilian movement of digital rights, Data Privacy Brasil Research Association focuses on strategic plans that can improve the protection of fundamental rights, enhance the State's regulatory capacity and restrict abuses and discriminatory practices by the private sector.

For more information on the Observatory, go to **http://observatorioprivacidade.com.br**. For more information on the Data Privacy Brasil Research Association, as well as for access to the Ethical Funding and Transparency Policy, go to **http://dataprivacybr.org**.

Document License

Institutional Information

Data Privacy Brasil is a space of intersection between Data Privacy Brasil Ensino, a company that provides data protection courses and training, and Associação Data Privacy Brasil de Pesquisa, a non-profit civil association based in São Paulo. The organization is dedicated to research and advocacy on the interface between personal data protection, technology, and fundamental rights. Based on an Ethical Funding and Transparency Policy, the Associação develops strategic research projects, mobilizing knowledge that can help regulators, judges and law professionals deal with complex issues that require in-depth knowledge about how technologies and socio-technical systems affect fundamental rights. The Associação receives funding from international philanthropies such as the Ford Foundation, Open Society Foundations, and AccessNow, as well as domestic funders such as the Comitê Gestor da Internet (CGI.br). For more information, visit http://dataprivacybr.org.

Members of the Multistakeholder Committee

The Multistakeholder Committee was constituted by specialists from civil society and private companies that opined on a preliminary version of the report in April 2020. Participated in the Committee voluntarily: Bárbara Prado Simão (Brazilian Institute of Consumer Protection), Luiza Brandão (Institute For Research On Internet and Society), Francisco Brito Cruz (InternetLab), Piero Formica (Tim) and Raíssa Moura (InLoco). The views expressed in this report do not represent the views of the Committee members, who expressed themselves in their own individual capacities.

Consultancy for revision

The report was revised by Clara Iglesias Keller, post-PhD candidate at the Leibniz Institut für Medienforschung | Hans-Bredow-Institut and researcher associated to the Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG).

Authors

Bruno Ricardo Bioni
PhD candidate in Commercial Law and Master with honors in Civil Law at the Faculty of Law of the University of São Paulo (USP). Was a visiting researcher at the European Data Protection Board/EDPB and the Council of Europe Data Protection Department. Bruno was also a visiting researcher at the Research Centre for Law, Technology and Society of The University of Ottawa Faculty of Law and legal and a government relations adviser at The Brazilian Internet Steering Committee/CGI.br and the Brazilian Network Information Center/NIC.br. He integrates the Latin American Network of Surveillance, Technology and Society Studies/LAVITS. He is a professor and founder of Data Privacy Brasil.

Rafael A. F. Zanatta
PhD candidate at the Institute of Energy and Environment of the University of São Paulo (USP). Holds a Master's degree by the Faculty of Law of the University of São Paulo (USP). Holds a Master's degree in Law and Economy by the University of Turin. Alumni of the Privacy Law and Policy Course at the University of Amsterdam. Was the coordinator of the digital rights program of the Brazilian Institute of Consumer Protection – IDEC, a project lead at InternetLab and a researcher at FGV's São Paulo Law School - FGV/SP. Through IDEC, Rafael was a representative of the Anatel's Telecommunications Users Defense Committee and a member of the workgroup on Technology and Consumption of the Ministry of Justice. Integrates the Latin American Network of Surveillance, Technology and Society Studies/LAVITS. He is Data Privacy Brasil's research coordinator.

Renato Leite Monteiro
PhD candidate in Philosophy and General Theory of Law at the University of São Paulo (USP). LL.M in Technology Law by NYU and NUS. Was a visiting researcher and advisor at the Council of Europe Data Protection Department. Guest professor at several institutions such as USP, Mackenzie, FGV, and Insper. Has actively collaborated with the discussions and redaction of the General Data Protection Law - LGPD (in the Portuguese acronym). He is a co-chair, in Brazil, of the International Association of Privacy Professionals – IAPP, and holds CIPP/E, CIPM, and FIP certifications. Founder and Director of Data Privacy Brasil.

Mariana Rielli
Lawyer, graduated from the University of São Paulo (USP). Was a legal and advocacy advisor for ARTICLE 19 Brazil. Was an advisor for Alianza Regional por la Libertad de Expresión e Información. She is the leading project researcher at Data Privacy Brasil.

Translation

Giovana Trevisan Pigatto
Translator with BA in Languages at University Estadual Paulista.

Gabriela Machado Vergili
Researcher at Research Association Data Privacy Brasil. Law graduate at Catholic Pontificial University of São Paulo.

Institutional support

The elaboration of this report relied on the financial support of the non-profit entity AccessNow, based in the USA. For more information on the entity's role in the promotion of digital rights, go to http://www.accessnow.org/about-us/.

How to quote this document

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacy and pandemic: recommendations for the legitimate use of data in the fight against COVID-19. Translation: PIGATO, Giovana; VERGILI, Gabriela. São Paulo: Data Privacy Brasil, 2020.

Executive Summary

The Report *"Privacy and Pandemic: Recommendations for the legitimate use of personal data in the fight against COVID-19"* presents principles and recommendations to assist in the development of policies on personal data sharing between Public Administration and private sector entities, in the context of the International Health Regulations (adopted by Decree 10.212/2020) and of theAct 13.979/2020 (which establishes the measures for coping with the public health emergency caused by the COVID-19, also known as "Quarantine Act").

The Report's goal is to inform about the current decision-making procedures in Brazil, both in the public and private sectors, aiming to develop innovative solutions that concern data use[1] in order to help in the fight against one of the greater pandemics of the last century.

Regardless of the validity of Act 13.709/2018 (Brazilian General Data Protection Act – LGPD in the Portuguese acronym), the parties involved in actions of this nature own the duty of incorporating safeguards and risk mitigation mechanisms for fundamental rights, resulting from the Brazilian legal system. This duty can be extracted from the already diffused legislation in the country, acting like normative sources of the proposals contained in this report, besides the already mentioned International Health Regulations and Quarantine Act, the sectoral standards of personal data in force (such as the Act 12.965/2014 - Brazilian Civil Rights Framework for the Internet (MCI in the Portuguese acronym), the Decree 8.771/2016, the Act 12.527/2011 - Freedom of Information Act, the Act 9.472/1997 - General Telecommunications Act[2], among others) and the protective norms of fundamental rights guarded by the national legislation, especially the Brazilian Constitution of 1988 and other international treaties on human rights in which Brazil is a signatory.

1 In this report, we use the term "personal data" and "data" interchangeably for easy reading. In addition, it is important to stress that the concept of personal data follows an expansionist logic: information related to an "identified or identifiable individual". Therefore, personal data goes beyond the ID number, social security number, and address, and it may also be considered as location data - (e.g., geolocation data) or electronic identifiers (IP address, MEI, Mac address) if they are related to a person - article 14, of the Act 8.771/2016. In this regard, BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Grupo Editorial Nacional, 2020 (2nd edition).

2 Article 72. The service provider can use information relative to the user's individual utilization of services only in the execution of its activity. (...) Paragraph 2. The service provider can disclose aggregate information on the use of their services to third parties, as long as the information shared does not allow the direct or indirect identification of the user and does not violates their intimacy.

In this scenario, the LGPD, although still not in force[3], takes a guiding role in these public policies, since it represents a set of principles approved by the Brazilian legislator as fundamental for the constitutional approach on data protection in the national territory. This role does not depend on the validity of its deontic rules, and although the principles and recommendations of this report follow the established guidelines, its relevance waives the validity of the LGPD, deriving from the set of in force laws already mentioned.

What are the practical implications of this legal framework in the moment of data use for the fight against the COVID-19 pandemic? How does it affect and condition the practical conduct of public officials and private actors involved in the formulation of these measures?

Facing these questions, this Report by Data Privacy Brasil Research Association presents a series of recommendations on how the requirements of data access must be done, and what are the best practices for collaborative projects between companies and the different spheres of Public Administration. Despite its general character and applicability for several activities related to regulation and data processing, this development had the constitution of protocols for data processing as its focus, especially its shared use[4] in order to combat COVID-19.

As discussed in the Methodology, these recommendations are the result of an elaboration process of five steps that must be present on the institutional decision-making procedures related to the subject covered by the Report:

Step 1: Assessment of the need for data-centered health policy development

Step 2: Definition of purpose and need for data processing

Step 3: Definition of data life cycle and disposal

Step 4: Definition of specific safeguards for fundamental rights

Step 5: Assurance of publicity, transparency and participation

Along with these steps, a total of 10[5] principles[6] were identified in order to be observed on each

3 At the time of the publication of the report the Brazilian General Data Protection Act was not in force yet. It became in effect on September 18th, 2020.

4 In its Article 5, XVI, the LGPD defines shared use as: "communication, dissemination, international transfer, interconnection of personal data or shared processing of personal data banks by public agencies and entities, in compliance with their legal competences, or between these and private entities, reciprocally, with specific authorization, for one or more types of processing allowed by these public entities, or among private entities".

5 Besides the 10 principles, 8 sub principles were formulated, totaling 18 guidelines.

6 The formulation in principles is based on the understanding that these proposals constitute notions and fundamental values that must conduct the decision-making procedures related to the use and sharing of personal data in the fight against the COVID-19 pandemic. However, it is recognized that the theoretical discussion about what differentiates the principles as rules contains dissent

one of these steps by the public officials and private agents involved with them. The following principles are:

Principle 1: Reasoned motivation

Principle 2: Support in a legal authorization

Principle 3: Formalization in a legal instrument

Principle 4: Definition of an explicit and specific purpose

4.1. Prohibition of use for profitable ends and abusive discrimination

Principle 5: Limitation to the minimum necessary

Principle 6: Definition of data life cycle

6.1. Time limitation

6.2. Later exclusion to adequate use

6.3. Data quality

Principle 7: (Pseudo)anonymization in order to guarantee low risks of re-identification of individuals

7.1. The commitment of non re-identification by the recipient

7.2. Prioritization of information (output) and non-transfer of data *(input)*

7.3. Inclusion of reliable third party recipients in case the aggregation of database becomes necessary

7.4. Non-disclosure of identities of the recovered, infected or suspects

Principle 8: Assurance of information security

Principle 9: Active transparency

Principle 10: Preference for open source applications and technologies

Based on this analysis and the identified principles, the Report presents, by the end of each step, a synthesis with concrete recommendations referring to that stage. Below, the set of these recommendations is highlighted individually:

and ambiguities that go beyond this work's scope. About these discussions, see: SILVA, Virgílio Afonso da. Princípios e regras: mitos e equívocos acerca de uma distinção. Revista Lationamericana de Estudos Constitucionais. v. 1, 2003. PEREIRA, Jane Reis Gonçalves. Interpretação Constitucional e Direitos Fundamentais. Saraiva: São Paulo, 2018. Furthermore, it is registered that this formulation should not be confused with the regulatory technique of "regulation by principles", whose relevance the document does not test or cover (about the technique, see BLACK, Julia. The Rise Fall and Fate of Principles Based Regulation. LSE Law, Society and Economy Working Papers, n. 17, 2010.)

- **Need for technical and scientific basis as to the need and efficiency of personal data use:** starting from a scenario in which the use of data to fight against COVID-19 may escalate, it must be guaranteed that such actions are motivated and endorsed on technical and scientific pieces of evidence as for the need and efficiency of the use of such information;

- **Need for law and other specific legal standards to endorse the cooperation between the public and private sector:** concerning the cooperation with the private sector, the provision of formal law for the adopted measures is necessary, given the principle of legal reserve. Furthermore, the detailing by a legal instrument that proceduralizes the shared use of data within the public sector itself and of this one with the private sector is recommended, conferring a greater degree of legal security to the arrangement;

- **All the employed measures must be guided by the least possible intrusion of privacy:** in case the use of individualized personal data becomes necessary, it must be supported by a robust legal foundation, backed by a legal precept that can evidence in a clear and evident way that such form of data collection and use is strictly necessary and that such a goal cannot be reached by any other less invasive and intrusive way.

- **Respect for the idea of a well-delimited purpose:** Each and every activity of data processing for the fight against COVID-19 must have a strictly delimited purpose, through the indication of which is the specific measure applied, and only use the necessary data to reach this purpose. From that, it is possible to verify if the considered data modeling minimizes and maximizes, respectively, the risks to privacy and the efficiency in the fight against the pandemic;

- **Each and every operation of data use for the Fight Against COVID-19 must have a beginning, middle and end:** each and every operation of data processing for the fight against COVID-19 must have a predefined life cycle with a beginning, middle and end, including specifications of applied techniques, of the data that will be collected and processed and further means of disposal. The public official must predict a determined lifetime and disposal, defined before the implementation of a collaboration project for the shared data use on the terms of Act 13.979/2020;

- **Measures to contain privacy risks must be articulated in all cases:** starting from the premise that each and every activity of data processing carries privacy risks to their subjects, containment measures for the possible collat-

eral damages must always be articulated. From (pseudo)anonymization techniques, passing through segregation or, at least, aggregation of database with filters (reliable recipients), to the establishment of robust information security measures, there are several necessary actions in order to guarantee the lowest possible risks for fundamental rights and freedoms throughout the whole cycle of data use;

- **Maximum transparency of the measures and their governance:** the public authority must proactively give maximum transparency to the agreements of data sharing through publications of what are the actions, generated data, and contractual arrangements of shared use in its transparency portals, for instance. Not only the data processing activities themselves, but, above all, their technical details and the decision-making procedures that have led to their adoption must be disclosed; and

- **Open-source technologies:** the solutions adopted by the public and private sectors must be preferably open-source, in order to ensure greater access, democratic participation, public scrutiny, and, ultimately, efficiency.

The application of these principles and recommendations must be materialized both in public policies at the federal, state, and municipal levels, as well as in voluntary practices. Its adoption can be formalized in Decree, interinstitutional ordinance or technical standard to be published by a competent body; or yet, through commitment letters and guidelines from the public or private sector, as well as agreements and similar instruments of administrative law.

Summary

Introduction

The COVID-19 pandemic, an infectious disease caused by the severe acute respiratory syndrome coronavirus 2 (SARSARS-CoV-2), has been mobilizing political, economical, and social actions of new proportions. In less than four months since its discovery in China, the disease has reached a million individuals, leading thousands to death, especially those with some type of comorbidity and at an advanced age. In this context, governments have created specific legislation to combat COVID-19, including isolation measures, quarantine, and social distancing, as well as data sharing between the public and private sectors aiming to base and monitor the containment measures.

In comparison to other critical moments for public health worldwide, what makes COVID-19 stand out is that it is being disseminated in an extremely digitalized and connected world, in which data are produced with unprecedented speed and volume. Computational models, especially those based on machine learning, have been showing themselves useful to the development of monitoring and tracking technologies and even predictions on the disease advance. Therefore, sharing citizens' data for those purposes becomes a point of interest for public managers.

In Brazil, the Federal Act 13.979/2020[7], known as "Quarantine Act", has determined criteria for the performance of the Ministry of Health, including the compulsory testing and mobilization of police forces to the fulfillment of the *isolation and quarantine* measures (which include the separation of ill or contaminated individuals, or of luggage, means of transport, goods or affected postal parcels, in order to avoid contamination or propagation of the coronavirus, and the activities restriction and separation, in the same terms, of suspect individuals). The legislation provides that this measures, that imply limitations of basic constitutional rights, such as locomotion and economic freedom, "may be determined based on scientific pieces of evidence and analyses of the strategic health information and should be limited in time and space to the minimum necessary for the promotion and preservation of public health". The legislation recognizes the respect towards dignity, human rights, and fundamental human freedoms, as recommended by Article 3 of the International Health Regulations produced by the World Health Organization (WHO) and adopted by Brazil through Decree 10.21/2020[8].

7 BRAZIL ACT 13.979, FROM FEBRUARY 6TH, 2020. Stipulates measures to confront the public health emergency of international concern resulting from the coronavirus, responsible for the 2019 outbreak. Available on: <http://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735>.

8 BRAZIL. DECREE 10.212, FROM JANUARY 30TH, 2020 Promulgates the revised text from the International Health Regu-

These Regulations pay special attention to the protection of personal data. Article 45 stipulates that health information must be kept confidential and be anonymously processed, respecting the limits provided by national laws. Its Paragraph 1 provides that the States may process personal data "when it becomes essential for public health risk assessment and management purposes", ensuring that personal data are (i) processed in a fair and legal manner, and without other procedures that are unnecessary or incompatible with such purpose, (ii) suitable, relevant and not excessive concerning this purpose, (iii) accurate and, when necessary, updated, thereby ensuring that all the reasonable measures will be taken in order to guarantee that inaccurate or incomplete data will be erased or rectified, and (iv) kept only for as long as necessary.

The legitimate processing of data is essential to the formulation of public policies and private initiatives for the fight against COVID-19. Understanding the population's behaviour can help the Public Authority anticipate demands and allocate resources, personnel, and containment measures more efficiently.

In this context, Article 6 of Act 13.979/2020 determines that "the sharing of essential data for the identification of infected individuals or under suspect of infection by the coronavirus between bodies and federal, state, district and municipal public administration entities is mandatory, with the exclusive purpose of avoiding its propagation". This rule extends to the private sector when the data are requested by health authorities, and in case of data sharing between companies and the government, full respect for dignity, human rights, and fundamental liberties must be observed, as it is also recommended by the International Health Regulations.

The incorporation of data protection principles is crucial to give effect to the International Health Regulations, which expressly mentions the need to respect national data protection laws. In this sense, safeguards, such as time limitation, exclusion after use, robust technical measures of anonymization, and prohibition of monetization of sensitive data or use for any other purposes besides the necessary for the fight against the pandemic must be guaranteed..

The recognition of dignity, human rights, and fundamental freedoms is deeply connected to the right of personal data protection, already acknowledged, by the Brazilian legislator through the General Data Protection Act (LGPD), and that may soon become a constitutionally affirmed right in Brazil[9]. In the current context of the pandemic, Act 13.979/2020 and other pertinent rules (e.g, Brazilian Civil Rights Framework for the Internet, Decree 10.212/2020) must be seen, before anything else, within the parameters of fundamental rights guaranteed on article 5 of the Constitution of the Republic, which assures, for Brazilian citizens and foreigners living in the country,

lations, agreed on the 58th World Health Organization General Assembly, on May 23rd, 2005. Available on: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10212.htm>.

9 Constitutional Amendment Draft n. 17/2019.

the inviolability of the right to life, liberty, equality, security and property, honor, freedom of assembly, etc.

In order to guarantee these constitutional assets, the use of essential data for the identification of infected individuals or individuals under suspect of infections, especially the sharing of data between companies and the government, needs clear parameters that can be inspired by the LGPD, approved in 2018 by the National Congress and sanctioned by the President of the Republic. Its basis on a set of principles connects clearly with Article 45 of the International Health Regulations and other applicable norms, serving as relevant parameters of action for legislators and the public officials in the face of the current sanitary emergency.

The LGPD enables and establishes procedures to the use of personal data in situations of emergency, of proven public interest, and imminent need to protect lives. At the same time, it gives legal security for such uses, mainly for the sharing of data between private and public entities. In this regard, the LGPD must not be seen as an obstacle for the processing of personal data for such purposes, but rather as a normative reference of the balanced way of doing it by protecting fundamental rights and freedoms and assuring the public health at the same time.

The use of personal data in Brazil, in or out of a pandemic situation, must be based on human rights[10], the free development of personality, dignity, and the exercise of citizenship by individuals. For this reason, most of the practices and principles suggested here have a transversal application for the use of data to inform public policies of different natures. In the current context, the correct application of Act 13.979/2020 must occur based on some basic principles, which result from a joint interpretation of the applicable legal instruments.

10 In the context of COVID-19, the international human rights entities have also been positioning themselves regarding data processing alongside other matters. In this sense, consult: Resolución 01/20. Pandemia y Derechos Humanos en las Américas. Comisión Interamericana de Derechos Humanos. Available on: <**http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf**>.

II Methodology and infographic

By observing the 5 (five) steps described in this Report, decision-makers will have elements of sequential and eliminatory analysis to decide on how to make legitimate use of personal data in the fight against COVID-19. It is a kind of a test concerning the legality, legitimacy, and usefulness of the measure.

The first two relate to the duo necessity-adequacy of the measure intending to make legitimate and less invasive data modeling. Once the data that will be collected is well defined, the two following steps address what the risk management actions should be during the processing of the data, as well as the definition of parameters on when it should be discontinued. Lastly, the fifth and final step runs through all the previous ones so that proper transparency is given in order to enable collaboration and public scrutiny. If the script is to be observed, the data use tends to minimize risks to the data subjects and maximize efficiency in the fight against the pandemic.

Under what conditions can I use data in the fight against COVID according to national and international standards?

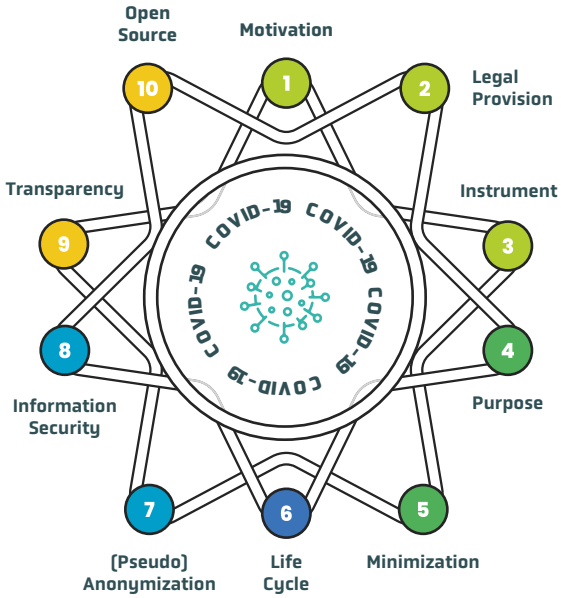
Step 1
Assessment of the need for data-centered health policy development

Step 2
Definition of the purpose and need for data processing

Step 3
Definition of data life cycle and disposal

Step 4
Definition of specific safeguards for fundamental rights

Step 5
Assurance of publicity, transparency and participation



Detailing the Principles...

Motivation: do I own scientific pieces of evidence that support personal data processing?

Legal provision: is there a provision for processing in law or regulation?

Instrument: is there a contractual or similar instrument?

Federal Constitution + International Health Regulations (Decree 10212/2020)

Purpose limitation: is there a delimited purpose?

Minimization: are the used data strictly necessary to achieve the purpose?

Data life cycle: a period of use and safe disposal has been delimited?

Quarantine Act, MCI (Brazilian Civil Rights Framework for the Internet) and Decree 8771/2016

(Pseudo)Anonymization: have appropriate techniques been applied to remove identifiers and elements of individualization?

Information Security: have the best security practices been observed?

MCI and Decree 8771/2016

Transparency: are the documentation and methods public and auditable?

Open Source: are the used codes subjected to public scrutiny?

Freedom of Information Act, CDC (Consumer Defense Code), Federal Constitution

"The thought-out design of data processing minimizes the risks to privacy and maximizes the efficiency in the fight against the pandemic."

III Principles and recommendations

From the joint interpretation of the International Health Regulations with the legal rules in force in Brazil, a set of principles that should guide the decision-making procedures in eventual cooperation agreements for the use of data in the fight against COVID-19 can be reached. These principles must be applied based on the five steps of the process of building these agreements, as set out below.

Step 1

Assessment of the need for data-centered health policy development

The first step consists of the decision on the shared use of personal data between Public Administration entities and between them and private sector entities. Such a decision can be formalized through a cooperation protocol, agreement, or requisition. This first step must follow the guidelines below.

Principle 1 *Reasoned motivation*

In order for the personal data processing to happen through access or shared use of data between public or private sector entities, it must occur in a fair and legal manner, with a clear need, as required by Article 45 of the International Health Regulations. This necessity must be demonstrated through reasoned motivation - a principle that rules the Brazilian public administration, according to Article 2 of the Act 9.784/1999. This principle aims to prevent the exercise of arbitrariness by the public official, requiring legitimate justification for intervention in the private sphere of the citizens[11].

Specifically, the motivation for the shared use of data whose controllers (responsible for) are private entities (e.g. telecommunication or technology companies) and/or public entities (e.g., ministries, autarchies, secretariats) requires:

11 SUNDFELD, Carlos Ari. Motivação do ato administrativo como garantia dos administrados. *Revista de Direito Público*, nº 75, 1985, p. 118.

(i) the exposition of the reasons why it is believed that a specific set of data is essential for the public health policy;

(ii) scientific or empirical evidence that the processing of this information is important for social distancing and other measures for the containment of COVID-19[12].

Generic requirements and discretionary acts cannot be admitted as a mere request for data sharing without the proper reasoning that attests to the necessity and efficiency of the measure.

The implementation of public policies in the field of technology is characterized by high complexity and uncertainty about the actual implications of the adopted measures. In this sense, in non-emergency contexts and where there is no imminent risk to the collective, these procedures must ideally be preceded by analyses of impact that assess the options of the public official in the face of the demand for intervention.

Within this scenario, the exposition of the reasoned motivation of the administrator's action becomes even more important. Especially now, when the circumstances require effective and efficient measures, public officials must present scientific evidence that supports the importance of applying certain data analysis techniques (*e.g.* contact tracing) and present reliable results from their use. These pieces of evidence must be part of the foundation that supports the Public Administration's intervention. The emergency situation does not mean that the Public Authority can exempt itself from the duty of motivation; on the contrary, it becomes even more important.

Principle 2 *Support in a legal authorization*

According to the principle of legal reserve, the obligation of data sharing from the private sector to the public sector must be under formal law (role accomplished in the current context by the Quarantine Act). Preferably, this obligation must be regulated by decree, in order for the data processing to proceed in coherence with what is required by the list of guarantees related to data protection.

In matters such as this, in which the potential for restricting fundamental human rights is high, the provision by an infra-legal regulation reinforces the legal certainty and the legitimacy of the adopted measure. Furthermore, a decision circuit with checks and balances, in this case between

12 We will not analyze the specific question of what "scientific evidence" means. It is known that the production of scientific articles, papers, and international collaboration by scientists and universities for the fight against COVID-19 has been massive. This knowledge must serve as support for decision-making. The argument that "there is no scientific knowledge" on the subject cannot succeed.

the Executive and Legislative branches, is guaranteed.

Bearing in mind that the public health is a common and competing competency between the Union, States, and Municipalities, requests for partnerships to share data with different entities of the federation tend to multiply and become diffused. In this sense, the support in legal reserve also aims to avoid abuses in the context of an escalation of requests[13].

The principle of legal authorization prevents broad interpretations of Act 13.979/2020. As an example, the thesis that Departments of Public Security are considered as a type of "health authority" and thus are able to exercise the right to request data in the context of Paragraph 1 from Article 6[14] is mentioned. In this case, the infra-legal standard fulfills the important role of clarifying which public administration bodies fit this concept. In this case, there is already applicable infra-legal legislation that requires a restrictive interpretation of the term "health authority". In addition to the parameters of the National Health System Act (Act 8.080/1990), there is Ordinance 1.139/2013 of the Ministry of Health, according to which "health authority" is "a competent body or public agent in the health area, with legal attribution in the field of surveillance and health care".

Principle 3 *Formalization in a legal or similar instrument*

Each and every shared use of data within the public sector itself and between the public and private sectors must be formalized through a legally established contractual or similar instrument. In addition to respecting legality, formalization allows that the principles and consensual good practices stay registered[15].

Recommendations for Step 1: Starting from a scenario in which the use of data for the fight against COVID-19 may escalate, it must be considered that such actions are motivated and endorsed on technical and scientific evidence that account for the need and efficiency of the use of such information. Regarding the cooperation with the private sector, there must be protection on formal law, considering the principle of legal reserve, as well as regulation by secondary rules (which would proceduralize the shared use of data within the public sector itself and the public sector and private sector).

13 It is emphasized that the legality principle also works as a guarantee to private agents who do not wish to establish voluntary partnerships of data sharing.

14 "Art. 6 The sharing between public bodies and federal, state, district and municipal public administration entities of essential data for the identification of infected individuals or suspects of infection with the coronavirus is mandatory, with the sole purpose of preventing its propagation. § 1 The obligation referred to in the caput of this article is extended to private legal entities when the data are requested by a health authority.

15 For instance, this is the logic established by the LGPD when providing that the transfer and shared use between the Public and Private Sector, as well as data processing by the public administration, must be provided or supported by contracts, agreements or similar instruments (systematic interpretation between Article 7, III and Chapter IV).

Step 2
Definition of the purpose and need for data processing

Once the foundation and relevance for the personal data use have been defined according to the best available scientific evidence, as well as the legal-infralegal protection and the draft of a possible adequate legal instrument, a second step is the definition of the precise purpose of personal data processing. The explicit definition of the purpose is essential to ensure that the processing is "adequate and not excessive", according to article 45 of the International Health Regulations. To be adequate and not excessive, data processing depends on the clear definition of a purpose, consistent with the basic principle of purpose limitation (established on the Article 6, I of the LGPD and known in international law as *purpose limitation*).

Principle 4 *Definition of an explicit and specific puporse*

A logical consequence of any reasoned request is that the purpose of data processing is specified. In this sense, it is not enough to just mention the data processing in a generic way, like to *avoid the COVID-19 propagation*. But also the specific measure that is being considered must be pointed out. For instance, in addition to social distancing, the most commonly adopted practice today, there are others under discussion for the tracking of infected individuals and of the virus itself. Each one of the strategies must be justified, and with this, its adequacy must be verified[16] in relation to the requested data set. As a result, any use of this information for later purposes that are not exclusively related to the fight against COVID-19 in cities where there are confirmed cases is prohibited.

This mitigates the risks that the data used to combat the pandemic is used for discriminatory or exclusionary purposes, or that it influences individuals' access to public and private goods and services (which applies to a variety of situations, such as mobility in public spaces or future contracting of health and safety services).

The express and precise delimitation of the purpose needs to be included in the legal instrument that is part of the sharing agreement, such as a contract or cooperation term (Principle 3), precisely defining what the purpose of data processing will be (e.g. construction of cartographic analysis of agglomerations for inferences on most affected regions that may require investment in hospital beds and Intensive Care Units). This explicit definition is crucial to a later control of purpose deviation, which is prohibited by the International Health Regulations and by the standards of personal data protection.

16 This is the normative content of the adequacy principle in the LGPD - article 6, II: "compatibility of the processing with the purposes communicated to the data subject, in accordance with the context of the processing."

4.1 *Prohibition of use for profitable end and abusive discrimination*

The possibility of profitable partnerships by companies obtained from the shared use of data with public authorities in the context of the fight against COVID-19 must be absolutely prohibited. There cannot be profitable interests in the use of health information, which is considered sensitive personal data, to combat COVID-19.

It is the role of Public Authorities to ensure that the data processing is exclusive to the public interest, for non-profit purposes, to combat COVID-19. Partnerships and data lake arrangements cannot have "access fees" from private companies responsible for their organization.

Likewise, and as already mentioned in this Principle, the data processing for discriminatory purposes that are illegal or abusive must be prohibited, in obedience to the equality principle, established in the 5th, caput of the Federal Constitution, verticalized on Article 6, item IX, of the LGPD and, finally, expressly repeated in Article 42 of the International Health Regulations.

Principle 5 *Limitation to the minimum necessary*

Policies to contain the COVID-19 propagation and to monitor the impact of the disease should be made by minimizing data collection. Only data that is strictly necessary for the accomplishment of the intended purpose must be collected and used[17] in order to avoid mass data collection, which may have an undesirable impact on fundamental rights. One of the ways to implement this principle is the use of mechanisms of "self-assessment" of the population through Unstructured Supplementary Service Data (USSD), GMS technology that allows the population to respond to some questions in an agile protocol, which does not require personal data collection. Whenever possible, the public official should opt for less invasive technical solutions that are appropriate for the intended purposes. The mentioned principle minimizes risks to privacy and other fundamental rights at the same time that it maximizes efficiency, by concentrating information processing capacity in a smaller quantity of quality data.

Technical solutions for contact tracing based on the exchange of keys and random IDs generated by Bluetooth (technology of contact exchange by proximity), that dismiss the collection of geolocation data and unique identifiers of the device, can be options to limit the data to the necessary minimum, which must be assessed in each case.

17 The principle of minimization is already in force on the Brazilian legal framework (e.g., Article 13, § 2nd, of Decree 8771/2016), having been systematized by the LGPD in its Article 6, III: "limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing".

Recommendations for Step 2: Each and every data processing activity aimed at the fight against COVID-19 must have a strictly delimited purpose, through the indication of which the specific measure is, and only use the necessary data to reach such purpose. From that, it is possible to verify if the considered data modeling minimizes the risks to privacy and fundamental rights and maximizes the efficiency in the fight against the pandemic.

Step 3

Definition of life cycle and disposal

Once the purpose for the data processing is precisely defined, as well as whether the data are indeed necessary for the intended public policy goal, companies and governments must define the time period of the cooperation. And most importantly, they must define the data life cycle, which means the beginning, middle and end of its processing. In this step, the observation of "not kept longer than necessary" rule from the International Health Regulations (Article 45, 2, d) gains relevance.

Principle 6 *Limitation to the minimum necessary*

Each measure for the COVID-19 fight and its respective data processing activity must have an expiration date by which it is conceived, implemented, and finally, discontinued. This is already an obligation in force in the Brazilian legal framework, as in the case of the provisions of Article 13, § 2, I, of Decree 8.771/2016. A cycle through which data are collected, used, and disposed of when its purpose is accomplished, which can be given by the pandemic control as a whole or by the success of a specific adopted measure.

It is recommended that a "life cycle plan", in a macro sense, is elaborated as an attachment to the technical documentation of cooperation between public and private authorities. This means that, in addition to the information on which data will be shared, the systems and file formats, as well as which (pseudo)anonymization techniques will be used must also be established.

6.1 *Time limitation*

The data processed to instrumentalize public health policies and new ways of containment of the COVID-19 propagation must be used not only with purpose delimitation but also with a clear time limitation. The data processing for undetermined time must be prohibited.

For instance, the use of data for applications of contact tracing and automatic notifications by SMS or USSD must have a clear time limitation, parameterized accordingly to the legal norms that define the quarantine period and the more rigorous measures by the Public Authority. The pandemic situation will not last forever and it is not acceptable for the data to be used without a clear prediction of its end. In this sense, the cooperation terms for shared use of data must be seen from the perspective of a project, with a beginning, middle, and end.

In case of the need for data analyses for longer periods, due to the performance of collaborative scientific studies (e.g. modeling of the spatial dynamics of the epidemic and assessment of the social distancing impacts), the definition of the time of data processing must be defined in technical and scientific evidence, in a reasoned manner and in harmony with Principle 1.

Once the COVID-19 crisis is over, the government is obligated to delete the data required by legal entities under private law, preventing its reuse and transfer to other databases inside the Public Administration. The State has to promote the exclusion of this information.

The legal instruments that deal with data sharing between public administration or private sector entities can provide for auditing after the period of data processing, in order to confirm their exclusion.

6.1 Data quality

In line with the provisions of Article 6, V, of the LGPD, Article 45 of the International Health Regulations, determines that data be accurate and, when necessary, that they are kept updated. In this process, the adoption of reasonable measures in order to ensure that inaccurate or incomplete data are erased or rectified was also provided for. In this regard, the principle of data quality favours the legitimacy of decisions made based on such data, making them consistent with reality and restricted to relevant data.

Recommendations for Step 3: Each and every operation of data use for the fight against COVID-19 must have a beginning, middle and end, so that the data are collected, used, kept updated and accurate, and in the end, discarded. The public official must formulate a plan for the data life cycle, providing for useful life and disposal. This includes the provision of processing stages and techniques, in addition to express time limitation.

Step 4
Definition of specific safeguards for fundamental rights

According to Article 3 of the International Health Regulations, it is crucial to adopt measures that safeguard "fundamental human freedoms", once the specific purposes and techniques of minimization are defined and a plan for data life cycle describing the duration and exclusion measures is constructed. This protection is achieved through a series of safeguards, which can be operationalized based on a set of principles to be followed by the involved agents,

Principle 7 *(Pseudo) Anonymization in order to guarantee low risks of re-identification of individuals*

Any data processing must, whenever possible, go through a technical stage that prevents the identification of individuals to whom they originally referred, which is commonly known as anonymization[18]. (Pseudo)anonymized data are the ones that can be re-identified through a combination with other databases, based on reasonable efforts[19], while still being personal data. For instance, geolocation data are, as a rule, considered (pseudo)anonymized to the mobile operators, since they own the capacity of identifying the individuals to whom they refer to, individually.

According to what specialized literature teaches us[20], it is not possible to ensure data that is, at the same time, 100% useful and 100% anonymized. Besides, the high probability of re-identifying mobile location data, including the supposedly anonymized ones[21], through statistical and grouping methodologies is known. For these reasons, the goal of public policies and sharing agreements must always be to ensure the highest possible level of (pseudo)anonymization. In this regard, whenever opening or making shared use of (pseudo)anonymized databases is considered, it should be made explicit what the respective techniques are and, preferably, there should be testing in order to

18 On anonymization and related subjects, BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 191-201, Janeiro-Março/2020. Available on: <https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902>,

19 See Article 12 of the LGPD and, in terms of comparative analysis, recital 26 of the General Data Protection Regulation.

20 UBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization and Risk. *New York University Public Law and Legal Theory Working Papers* 530, 2015.

21 ZETTER, Kim. Anonymized Phone Location Data Not So Anonymous, Researchers Find. 2013. Available on: <https://www.wired.com/2013/03/anonymous-phone-location-data/>.

measure their resilience level.[22] [23]

It is important to give preference to techniques that provide the highest possible level of anonymization. For example, whenever initiatives such as heat maps are considered, it is recommended to increase the mapping area to cover as many properties as possible, avoiding the granularity of the information. In addition, the frequency of data updates to cover more events, and thus, hinder the identification of a recent case (individual or group of individuals who disobeyed social isolation) can also be reduced. All of these measures hinder the reversal of the (pseudo)anonymization process.

The anonymization or (pseudo)anonymization techniques presented in collaborative projects (e.g. construction of Social Isolation Indexes through cartographic analyses) must go through a rigorous evaluation process, preferably by peers in the scientific and computer science and data community.

The government should promote public calls and awards so that researchers and computer scientists can demonstrate the failures in (pseudo)anonymization procedures, evidencing cases in which the re-identification of individuals is possible, posing risks to public liberties. Ideally, these calls could be considered mandatory as a "trial period" in order to condition the full implementation of the data-sharing project based on this cooperation. In case there is no time to hold such events, it must be allowed for external entities to test the robustness of the shared databases, and it is up to the Public Authority and private entities to develop environments in which such re-identification attempts can be performed using tools and techniques chosen by those responsible for the tests.

7.1 *The commitment of non re-identification by the recipient*

In case there is use of or mere access to (pseudo)anonymized data, the recipient must commit not to do, or try to do, any type of reverse engineering or procedure that leads to the re-iden-

22 In this regard, one of the practices for evaluation through the Privacy Maturity Model, created by the American Institute of Certified Public Accountants and by the Canadian Institute of Chartered Accountants (AICPA/CICA), is the optimization, i.e. "periodic revision and evaluation are used in order to ensure continuous improvement of a certain procedure". Available on <https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf>. The application of this analysis model (and compliance specifically to this practice) was observed in the personal data processing carried out by the municipality of Seattle. See: Future of Privacy. City of Seattle: Open data risk assessment, 2018. Available on <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>.

23 An example of the difficult balancing dynamics in the use of anonymization methods to combat diseases has occurred in the context of the fight against Ebola. In Sean Mcdonald's article (MCDONALD, Sean Martin. Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. CIS Papers 2016.1.), the author explores how the use of contact tracing data, in the case of the disease, was more effective based on data re-identification, that is, from an identifiable and individualized data basis. Although it was possible, anonymization was not even useful for the intended purpose. Kendall, Kerry, and Montjoye's warning, according to which "the best practices must accept that there are no perfect ways to anonymize data and there will probably never be" is also noteworthy. (KENDALL, Jake; KERRY, Cameron F. e MONTJOYE, Alexandre de. Enabling Humanitarian use of Mobile Phone Data, Technology Innovation, November 2014. Available on: <http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enablinghumanitarian-mobile-phone-data/brookingstechmobilephonedataweb.pdf>.

tification of the data subjects, even if they own the necessary methods and techniques to do so. This obligation must be expressly stated in a contractual or similar instrument, in a way that does not prevent members of the technical and scientific community from testing the robustness of the (pseudo)anonymization procedures.

7.2 *Prioritization of information (output) and non-transmission of data (input)*

When sufficient to meet the public policy goal, the transfer of information must be prioritized over the transmission of data.

In order to accomplish several of the actions against COVID-19, such as social distancing, agents from the private sector (e.g, telecommunication and technology companies that own the geolocation of individuals) do not need to transmit such data, in raw form, to the health authorities. It is enough that they process the data themselves internally and reveal the information resulting from these procedures, such as the neighbourhoods, regions, or even cities and states that are obeying measures to restrict mobility. This is the case, for instance, of the so-called "heat maps", that technically prevent any access to personal identifiers, such as IMEI, device ID, or precise tracking of individual device movements. In this regard, location data - whether obtained through GPS, data triangulation, or other contemporary techniques - would not, in theory, have the potential to identify a specific individual.

The principle of prioritizing information (output) can also be applied if awareness campaigns on specific neighbourhoods or regions become necessary. If the private sector agents already own a point of contact with the subject, they can perform mass messaging themselves, instead of transferring data from their users to the health authority to do so.

7.3 *Aggregation of database and reliable recipients*

For some actions, the combination of databases (*input*) to extract information (*output*) may be necessary, for example, to identify the effectiveness level of a medicine. In this case, in order to construct a representative sample - patients with different genetic characteristics and social-economic conditions -, the aggregation of databases from different hospitals, public and private, may be necessary.

In order to preserve the fundamental freedoms and rights, third parties - "reliable recipients" - can be elected to manage the hospital data in possession of this information and with an interest in combining them. These reliable recipients could also act on the anonymization of these data, including on the effectiveness metrics of the medicine (taking the example

previously mentioned). The companies may require recipients to sign a Term Sheet to the Principles in this report.

In addition to reliable recipients, probabilistic data structures can be used. These structures preserve some properties of the data at the same time that they increase the anonymization level. The HyperLogLog (HLL), for example, is a probabilistic data structure that aims to collect efficient information from a set without identifying the individual in the set. It is possible to calculate the cardinality (numbers of things with no repetition) of the set and make joins with other HLLs. This technique can also be used, for instance, to analyze the capacity of hospitals in order to avoid overcrowding, through the precise counting of visits, extracted from location data, without identifying individuals[24].

7.4 *Non-disclosure of identities of the recovered, infected or suspects*

Specific measures to prevent propagation are not to be confused with disclosure of information from individuals who have contracted COVID-19 and recovered. There is still no scientific information on COVID-19's impact on the respiratory system. Therefore, the presentation of personal information from those who have recovered may pave the way for abusive and discriminatory uses of these data by third parties.

As decided by the Supreme Court of Israel[25], it is recommended that individualized analysis measures are restricted to infected individuals, and the implementation of surveillance measures to all the suspected individuals is prohibited, under the risk of reversing the constitutional logic of primacy of the civil liberties in a democratic system and establishing a permanent environment of surveillance without due legal procedure.

This concern is also present in initiatives such as the TraceTogether application, implemented in Singapore[26] and in other pilot projects built in Italy that use techniques of non-personal identification of the infected, based on solutions such as the analysis of information obtained

24 WEBER, Griffin M. YU, Yun William. HyperMinHash: MinHash in LogLog space. Journal of Latex Class Files, Vol. 14, no. 8, August 2015. Available on: https://arxiv.org/pdf/1710.08436.pdf, TSCHORSCH, Florian, VON VOIGT, Saskia Nuñez. RRTxFM: Probabilistic Counting for Differentially Private Statistics. Available on: <https://eprint.iacr.org/2019/805.pdf>. ALAGGAN, Mohammed; GAMBS, Sébastien; MATWIN, Stan, TUHIN, Mohammed. Sanitization of Call Detail Records via Differentially-Private Bloom Filters. 29th IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC), Jul 2015, Fairfax, VA, United States. pp.223-230, ff10.1007/978- 3-319-20810-7_15ff. ffhal -01745827, BASIN, David; DESFONTAINES, Damien; LOCHBIHLER, Andreas. Cardinality Estimators do not Preserve Privacy. 2018. Available on: <https://arxiv.org/pdf/1808.05879.pdf>.

25 With Knesset Oversight in Place, High Court Greenlights COVID-19 Surveillance, JNS, March 26th, 2020. Available on: <https://www.algemeiner.com/2020/03/26/with-knesset-oversight-in-place-high-court-greenlights-covid-19-surveillance/>.

26 There is no scientific evidence on the positive impact of TraceTogether, formulated by the Singapore government. However, it is a public policy experience with wide notoriety.

through smartphone communication protocols. Measures like these must be prioritized, in order to avoid the disclosure of personal information[27].

Principle 8 *Assurance of Information Security*

As data processing is intensified, including through the expansion of individuals and entities that can access a database, it is essential to adopt identity management systems that prevent security incidents. There must be not only authentication mechanisms but also the creation of detailed inventories on who had access to which database, what data were accessed, when such access happened, and its duration. For instance, in the self-monitoring hypothesis, which can be done through an application downloaded by the citizen itself, the data must be stored on their device and properly encrypted, as is being developed in the European Union[28].

To illustrate this, the minimum information security requirements are legally supported, in a transversal way, in Section II - Standards of security and confidentiality of records, personal data, and private communications - of Chapter III of Decree 8.771/2016, on a sectorial manner in the financial sector, in Resolution 4.658/2018, and, based on the provisions of Resolution 2/2020 of the Central Data Governance Committee[29]. This security parameters may be increased from the compliance with information security standards, such as the NIST[30] or specific ISO standards.

27 The "Coronavirus Outbreak" project in Italy prioritizes the analysis of data exchanged by the "Bluetooth LE handshaking protocol" of smartphones anonymously. On the subject, Dave Mosher, 'A new phone-tracing technology could tell if you've been exposed to the coronavirus — without sacrificing privacy. 130 researchers are offering it to countries for free', Business Insider, April 4th, 2020. Available on: <https://www.businessinsider.com/coronavirus-covid-19-contact-tracing-mobile-phones-bluetooth-pepp-pt-2020-4>.

28 An initiative called Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) intends to implement the contact tracing technique without compromising privacy. According to the creators, the idea is that the application creates temporary IDs that will communicate via Bluetooth, without the need for the company to store any data. Source: An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contact tracing, TechCrunch, April 1st, 2020. Available on: <https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/>.

29 The mentioned resolution establishes rules for the sharing of data and security requirements that must be observed by the bodies and entities of the direct, autonomous and foundational federal public administration and by several other Union authorities. In its General Clause, it establishes that the data processing performed by third parties (hired companies) must also respect the security controls established in the document. Several public notices are being opened for the hiring of Startups that develop solutions to combat COVID-19, but these companies must have a sufficient level of maturity in information security to process personal data, including sensitive data, in the exceptional context of the pandemic, respecting the minimum information security requirements.

30 NIELES, Michael, DEMPSEY, Kelley L., PILLITTERI, Victoria Y. An Introduction to Information Security. Special Publication (NIST SP). Available on: <https://www.nist.gov/publications/inoduction-information-security>.

Recommendations for Step 4: Based on the premise that each and every data processing activity carries risks to privacy and fundamental rights of its subjects, measures of containment to these possible collateral damages must always be articulated. From (pseudo)anonymization techniques, passing through segregation or, at least, aggregation of databases with filters (reliable recipients), reaching the establishment of robust information security measures, there are several necessary actions in order to guarantee the lowest possible risks throughout the whole cycle of data use.

Step 5
Assurance of publicity, transparency and participation

The delimitation of specific purposes, minimization, life cycle, and specific safeguards to fundamental rights are not enough for the legitimate personal data processing in the fight against COVID-19, in compliance with international and national legal framework. One final fundamental step, that presents itself as a procedural requirement to be observed throughout the other stages, is the one of publicity and transparency of these procedures. In addition to giving legitimacy to the procedure, in obedience with the Federal Constitution and the Access to Information Act, it ensures that health measures are applied "in a transparent and non-discriminatory manner", according to Article 42 of the International Health Regulations.

Principle 9 *Active transparency*

The active transparency principle means that not only the data processing activities but, above all, their technical details must be made public. This translates as a "transparent" management[31] of what is done with the personal data as a pillar for actions to combat COVID-19.

The transparency principle is already in force in the Brazilian legal framework (e.g., Article 37 of the Federal Constitution; Article 31, caput, of the Freedom ofInformation Act, Article 7th, III, of the MCI), having been reinforced by the LGPD in its Article 6th, VI: "data subjects are guaranteed clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy".

The active transparency principle means that private entities and public authorities must be proactive in providing clear, adequate, and easily accessible information about what information is used,

31 Article 31, caput, of the Freedom of Information Act: "Article 31. The processing of personal information must be done transparently, and with respect to intimacy, private life, honor, and image of individuals, as well as individual freedoms and guarantees".

for which purposes, and who are the agents involved in the data processing chain. While the public authority must publicize such actions and the respective contracts for shared use of data on transparency websites, the private sector must maintain, preferably on the internet, not only the list of initiatives, but also the terms of its cooperation protocols.

Principle 10 *Preference for open source applications and technologies*

The principle of preference for open source applications and technologies implies that the government should favor solutions without proprietary codes - which means, that are not the property of any specific private agent and that are openly accessible. Ideally, technological solutions and new applications are managed and supervised by a civil group that has experience in open source.

International experiences demonstrate the importance of an open data policy. In the case of TraceTogether, it was built from an eight-day coding marathon, and today it is used by 1 in each 5 Singapore residents for contact tracing policies. The generic source code is called OpenTrace and it can be implemented on iOS and Android systems. The BlueTrace protocol, from which OpenTrace and TraceTogether operate, has also been made available entirely in open source. According to what was announced by the Singapore government, "the OpenTrace code source will be maintained by a group of open-source activists. As a governmental body, GovTech has decided to put the code in open source so that any improvements in OpenTrace are always available for free so that others can implant and improve. It also allows the users to evolve the codebase to suit the local context"[32].

Preferably, in order to facilitate public scrutiny, open-source technologies must be adopted so that the community can evaluate such tools and, above all, contribute to their improvement. Furthermore, interoperable standards of data sharing must be adopted, to make the use by several actors more efficient and less expensive.

Recommendations for Step 5: Transparency measures not only allow social control but also the collaboration of society itself to think about and improve measures to fight COVID-19. In the case of Public Authorities, transparency must be held proactively through publications of what the actions are, the data that is generated and contractual arrangements for shared use in its transparency websites, for example. Also, the solutions adopted by the public and private sectors must preferably be of open source software, in order to reduce operation costs, increase the program's efficiency, and allow the public scrutiny of technology.

32 6 things about OpenTrace, the open-source code published by the TraceTogether team, GovTech Singapore, April 9th, 2020. Available on: <https://www.tech.gov.sg/media/technews/six-things-about-opentrace>.

IV Conclusions and final recommendations

Regardless of the validity of the General Data Protection Act (Act 13.709/2018), the International Health Regulations (Decree 10.212/2020) and the Quarantine Act already bring clear rules on data protection applicable to the measures taken within the context of the fight against COVID-19. These provisions must be interpreted in accordance with the Federal Constitution, among other existent laws and regulations, in order to inform decision-making on the sharing of personal data between private agents and public authorities.

If the recommended principles and good practices of data protection are internalized and well implemented, the probability of efficiency of these measures will be higher, while also ensuring their legitimacy and providing greater trust for society. The personal data processing is just one of the containment measures to the COVID-19 pandemic, that must be conceived as such in order to be a proper containment measure and not the expansion of damages caused by the epidemic. The set of recommendations above makes clear that data protection is not a rival to this objective, but rather allows the State to be effective in the fight against the epidemic respecting the fundamental rights and guarantees of the population. In this regard, the Report highlights the principles that must be followed by regulators in the context of these decision-making procedures.

The COVID-19 crisis will pass, but the effects of the choices made by governments and companies may have long-term effects. In this sense, the use of technology and data must be held in a way that does not compromise fundamental rights, especially privacy and personal data protection.

In face of the LGPD's not being in force, the parties involved in agreements of personal data sharing have the duty of incorporating safeguards and mechanisms to mitigate risks to public liberties and fundamental rights, following the legislation already in force that is described in the present work.

In this Report, a concrete unfolding of this legislation was presented, in the form of five steps to be followed by public officials who are facing such agreements. The steps then are derived into a total of 10 principles. The recommendations extracted from this methodology can be implemented by public officials, civil society (third sector and academia) or internalized by professionals from private companies who lead data use initiatives for cartographic analyses, contact tracing, social isolation indexes, and other techniques for COVID-19 containment that are discussed worldwide.

For the authorities and public agents of the Federal Government and State and Municipal Governments, with competency to act on the matters covered by this Report, it is recommended:

- The creation of protocols based on the five steps presented in the Report:

  Step 1: Assessment of the need for data-centered health policy development

  Step 2: Definition of the purpose and need for data processing

  Step 3: Definition of data life cycle and disposal

  Step 4: Definition of specific safeguards for fundamental rights

  Step 5: Assurance of publicity, transparency, and participation

- The observation of the 10 principles presented in this Report, which are expressed on the formulations below:

  Principle 1: Reasoned motivation: is there any piece of scientific evidence that demonstrates the importance of implementing this data analysis technique to the fight against COVID-19?

  Principle 2: Support in a legal authorization: is there a clear definition of who the health authority is and identification of the legal standards that support the policy?

  Principle 3: Formalization in a legal instrument: is there a legal or similar instrument of administrative law to instrumentalize the data-sharing practice?

  Principle 4: Definition of an explicit and specific purpose: is there a clear definition of how the data will be used and to what specific purpose?

    4.1. **Prohibition of use for profitable ends and abusive discrimination:** does the agreement prohibit the use of data for profitable purposes as well as for discriminatory or abusive purposes?

  Principle 5: Limitation to the minimum necessary: has the technical team evaluated if there are less invasive ways of producing strategic information, by collecting the minimum of personal data?

  Principle 6: Definition of data life cycle: was there a definition of a detailed plan about the applied techniques, lifetime, and ways of disposal?

6.1. Time limitation: is there a clear definition of time limitation and scientific pieces of evidence on the length of use for studies?

6.2. Exclusion after the adequate use: is there an agreement on securely excluding data after specific use for the public policy?

6.3. Data quality: are there protocols for maintaining data accuracy and updating?

Principle 7: (Pseudo)anonymization controlled by the peers: have the (pseudo) anonymization techniques been validated by the technical and scientific community in order to ensure low risks of re-identification of individuals?

7.1. Prioritization of information: were forms of information analysis tested without the need to share raw data and original databases?

7.2. Aggregation of database and reliable recipients: in the case of database aggregation, are there conditions for the identification of reliable recipients who act as intermediaries?

7.3. Non re-identification commitment: is there a commitment on the part of those who will have access to the data of not applying engineering to try to revert the anonymization procedure?

7.4. Non-disclosure of identities of the recovered, infected, or suspect individuals: are the contact tracing and individual monitoring techniques restricted to the individuals infected with COVID-19?

Principle 8: Assurance of information security: are there information security protocols to minimize the risk of security incidents?

Principle 9: Active transparency: is there publicity for technical documents and wide transparency on the data processing techniques and system design?

Principle 10: Preference for open source applications and technologies: is it possible to adopt open source solutions, ensuring greater participation and security?

It is recommended for the Federal, State, and Municipal Executive Authority:

The elaboration of a Technical Note, in order to be published by Ministerial or Inter Ministerial Ordinance or similar, with the incorporation of the 10 principles as a way of interpreting, in a systematic way, the applicable legislation to eventual agreements on data sharing (whether between public administration bodies or private agents).

It is recommended for the Legislative Authority at the state level to adopt the 10 principles, ideally in an express manner, in the approved legislative texts that address data protection matters, as well as adopted measures in the context of the fight against the COVID-19 pandemic.

It is recommended for the private sector and civil society agents (academia and third parties) involved in decision-making procedures or partnerships of data sharing agreements: the voluntary adoption of the practices and principles listed in this document.

References

6 things about OpenTrace, the open-source code published by the TraceTogether team, GovTech Singapore, April de 9th, 2020. Available on: <https://www.tech.gov.sg/media/technews/six-things-about-opentrace>.

An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contact tracing, TechCrunch, April 1st, 2020. Available on: <https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/>.

Future of Privacy. City of Seattle: Open data risk assessment, 2018. Available on: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>.

Resolución 01/20. Pandemia y Derechos Humanos en las Américas. Comisión Interamericana de Derechos Humanos. Available on: <http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>.

With Knesset Oversight in Place, High Court Greenlights COVID-19 Surveillance, JNS, March 26th, 2020 Available on: <https://www.algemeiner.com/2020/03/26/with-knesset-oversight-in-place-high-court-greenlights-covid-19-surveillance/>.

ALAGGAN, Mohammed; GAMBS, Sébastien; MATWIN, Stan, TUHIN, Mohammed. Sanitization of Call Detail Records via Differentially-Private Bloom Filters. 29th IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC), Jul 2015, Fairfax, VA, United States. pp.223-230, ff10.1007/978- 3-319-20810-7_15ff.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 191-201, Janeiro-Março/2020. Available on: <https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902>.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Grupo Editorial Nacional, 2020 (2a edição).

BLACK, Julia. The Rise Fall and Fate of Principles Based Regulation. LSE Law, Society and Economy Working Papers, n. 17, 2010.

KENDALL, Jake; KERRY, Cameron F. e MONTJOYE, Alexandre de. Enabling Humanitarian use of Mobile Phone Data. Technology Innovation, Novembro de 2014. Available on: <http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enablinghumanitarian-mobile-phone-data/brookingstechmobilephonedataweb.pdf>.

MCDONALD, Sean Martin. Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. CIS Papers 2016.1.

NIELES, Michael, DEMPSEY, Kelley L., PILLITTERI, Victoria Y. An Introduction to Information Security. Special Publication (NIST SP). Available on: <https://www.nist.gov/publications/inoduction-information-security>.

PEREIRA, Jane Reis Gonçalves. Interpretação Constitucional e Direitos Fundamentais. Saraiva: São Paulo, 2018.

SILVA, Virgílio Afonso da. Princípios e regras: mitos e equívocos acerca de uma distinção. Revista Lationamericana de Estudos Constitucionais. v. 1, 2003.

SUNDFELD, Carlos Ari. Motivação do ato administrativo como garantia dos administrados. Revista de direito público , nº 75, 1985, p.

TSCHORSCH, Florian, VON VOIGT, Saskia Nuñez. RRTxFM: Probabilistic Counting for Differentially Private Statistics. Available on: <https://eprint.iacr.org/2019/805.pdf>.

UBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization and Risk. New York University Public Law and Legal Theory Working Papers 530, 2015.

WEBER, Griffin M. YU, Yun William. HyperMinHash: MinHash in LogLog space. Journal of Latex Class Files, Vol. 14, no. 8, August 2015. Available on: <https://arxiv.org/pdf/1710.08436.pdf>.

ZETTER, Kim. Anonymized Phone Location Data Not So Anonymous, Researchers Find. 2013. Available on: <https://www.wired.com/2013/03/anonymous-phone-location-data/>.