Studia Prawnicze. Rozprawy i Materiały 2021, nr 2 (29) • Studies in Law: Research Papers 2021, No. 2 (29)
ISSN 1689-8052 • e-ISSN 2451-0807

DOI: 10.48269/2451-0807-sp-2021-2-004

Vinicius Venancio Costa
Data Protection Lawyer in São Paulo, Brazil
ORCID: 0000-0003-0139-9183
vinicius.costa@fm.usp.br

Health data processing in the context of telemedicine: an overview between Brazil and the European Union post pandemic COVID-19

Introduction

The use of telemedicine had notably been developed in Brazil after the beginning of the public emergency period caused by the pandemic of COVID-19. In this context, health data are in the spotlight, since they represent the object and product of the health services provided, especially in the digital environment.

What measures has Brazil adopted to guarantee the data protection for health data in view of this scenario? The aim of this article is to examine and present a comparative analysis of the Brazilian and European Union regulations governing the processing of personal health data from a regulatory perspective, with the objective of highlighting possible differences and identifying elements that may converge towards a regulatory common denominator – if any – and to examine the potential actions to be taken at a national and international level between the regions.

The comparison with the EU was chosen due to the similar data protection regulation, since Federal Law No. 13709/18, the Brazilian General Data Protection Law ("LGPD") presents similar provisions and regulations to those established in the EU General Data Protection Regulation 2016/679 ("GDPR"), and by a study published on February 11, 2021 by the European Commission assessing the implementation of the GDPR and the domestic regulations for health data in each of the EU countries.[1]

[1] The creation of a European Health Data Space, is one of the Commission's priorities for the period 2019–2025, https://ec.europa.eu/health/ehealth/dataspace_pt [accessed: 23.04.2021].

This paper provides a brief evidence-based comparison of the situation regarding governance and regulatory aspects of health data in the aforementioned regions. The study the qualitative method with: (a) a review of the legal and regulatory literature to provide an overview of best practices; and (b) mapping and comparing the legal and technical aspects of health data use in order to establish an overview of the Brazilian legislation, regulation and governance models. The quantitative research method is not used in this article.

It is not the purpose of this article to establish in-depth reflections on the ways how data protection rights can be exercised in the regions in this study, nor the regulatory history with regard to the protection of privacy and the evolution of data protection in both regions – even though this aspect is tangential in view of its relevance, as well as the need to start from this point for the analysis of the subject.

Health data and their regulation in Brazil

The Federal Constitution provides broad language about the protection of the rights of privacy and private life of people (art. 5, item "X"), being the Federal Union competent to legislate about civil law (art. 22, item "I"), where privacy is included as a personal right, and Federal Union, States and Federal District are competent to legislate about the defense of health (art. 24, item "XII"). There is no explicit mention of "health data" in the constitutional charter. The regulation was left to infra-constitutional legislation, especially at the federal and state levels, as provided in the Constitution.

The LGPD was published on August 14, 2018 and comes into force gradually: the articles referring to the National Data Protection Authority (ANPD) became effective on December 28, 2018, the articles referring to the other provisions, including principles and security aspects, on September 18, 2020, and the articles referring to administrative sanctions will become effective on August 1, 2021.

Hence, we already have the first regulatory difficulty: there are provisions in force without any corresponding penalties.

The aim of the LGPD is to protect the fundamental rights of freedom and privacy and the free development of the personality of any natural person.[2] The LGPD establishes that "personal data" is any information relating to an identified or identifiable natural person, and may be classified as sensitive data, which is a special category of information that must be more strictly protected, with the LGPD providing a list of what is included in this category. In estab-

[2] As per article 1 of LGPD.

lishing what types of information constitute sensitive personal data, the LGPD refers broadly to "health data," without specifying what this concept means. The Brazilian legislation does not provide a specific definition of health data.

The second regulatory difficulty is presented: the lack of definition on what is considered "health data". Is it possible to affirm that this definition covers only medical exams, medical records and consultations related to a specific or determinable person? Would the data subject's biological monitoring data, or report management data, obtained via "wearables" be covered? Would the recording and scheduling of a patient's appointment with his or her physician constitute health data? These are some of the difficulties verified, which the legal interpreter should analyze in a case-by-case situation.

It is important to note that the regulations and guidelines of the LGPD are still under construction, discussion and analysis. The National Data Protection Authority (ANPD), structured under the Federal Decree No. 10,474 of August 26, 2020, and the creation of the Central Data Governance Committee, provided for in Decree No. 10,046 of October 9, 2019 are related.

There is a conflict of competence between those public bodies. The ANPD, created in the LGPD, is the supervise authority responsible for the protection of personal data in Brazil. Among its powers, the Central Data Governance Committee is responsible for the guidelines for the categorization of broad, restricted and specific data sharing. The Central Data Governance Committee was created after the enactment of the LGPD, under an administrative decree that is related to data sharing governance within the federal public administration.

Therefore, a third regulatory difficulty is noted: the competence for supervise powers of each body. Since telemedicine is a regulated activity, it should be noted that it is also subject to the federal and state medical councils, which, according to Federal Law No. 12.842/2013, has the Federal Council of Medicine as the competent authority to issue rules to define the experimental nature of procedures in medicine, authorizing or prohibiting its practice by doctors. The Federal Council of Medicine is also governed by Federal Law No. 3.268/57. If the topic is moved to telehealth, this regulation spectrum increases, since other professional councils, such as nursing, physical therapy, nutrition and speech therapy, shall be considered.

Thus, there are at least two competent bodies to regulate the matter: the provisions of the ANPD, and the provisions of the respective professional council. If the professional is also a member of the Federal Administration or has any relation with the Federal Administration, Central Data Governance Committee shall be called.

If the limits of the competence of each authority are not cleared, the liability regime established in the LGPD is also pending to be confirmed by judicial authorities and legal literature. The legal review has not reached a majority position whether the civil liability in the LGPD is strict or subjective.

In Brazil, civil liability is analyzed under: (I) the contractual aspect, which is studied on non-performance of contractual obligations, having the contract as its source; this means a violation of a duty dependent on the contract, and (II) the extra-contractual aspect, studied in the theory of unlawful acts, in which the duty to indemnify arises from the practice of an unlawful act, and might be based on the fault of the agent – being the subjective liability – or when the fault is not necessary to justify the duty to indemnify – when it is the strict liability.[3]

The classic rule of the civil liability states that it is subjective, and the volitional element must be considered. In strict liability, as an exception, the agent's guilt will not be analyzed in the harmful event, but only his act, and the causal relation for such, and it occurs, as provided in the sole paragraph of article 927 of the Brazilian Civil Code, whenever specified by law, or when the activity normally developed by the agent implies, by its nature, risk to the rights of others. Conceptually, in general terms, these are the differences between strict and subjective liability.

The consequence of defining whether liability for data protection is provided in LGPD, whether subjective or strict one, is the duty to consider any degree of lack of foresight, lack of skill or negligence of the agent in order to determine the obligation to repair the damage.

The LGPD provides in its article 42 that any agent who, due to the exercise of activities involving the processing of personal data, causes damage to others, in violation of the legislation for the protection of personal data, shall be obligated to repair it. There is no language determining that the liability would be "regardless of fault" – which could be argued that the law followed the general rule of liability, and therefore LGPD set the subjective liability as a rule.

On the other hand, when analyzing the liability exclusions in article 43, in the sense of agent's absence of conduct and/or illicit conduct that resulted in the damage, or if the damage was caused exclusively by a third party, the law excludes the duty to repair the damage. This means the agent shall demonstrate the lack of causal relation to the harmful event. In other words, there are strong elements to confirm that the liability is strict, and not subjective, since no mention to the guilty was made in the excluders. In addition,

[3] O. Gomes, *Civil Liability*, Forense, Rio de Janeiro 2011.

there are good grounds to determine the strict liability as per article 45 of the LGPD, that states in case of consumer relations, the liability rules provided in the relevant legislation should be applied; in this case the consumer legislation referred in the article determines the strict liability.

In any case this is another outstanding issue in regulation: the lack of definition of the liability regime in LGPD.

Hence, regarding health data in Brazil, there is no criteria formally defined to their definition. There are, for sure, situations that are easier to verify, such as information received by a health professional about a certain or identifiable person, or to the acts of a medical professional, in the terms of the CFM Resolution 1627/2001. However, in certain situations, the definition is not so obvious.

Data security measures, a key principle in LGPD, are the focal point of the regulation, especially when it comes to telemedicine, as developed below.

Telemedicine: regulatory overview

For historical purpose, the Ministry of Health established through Ordinance Act Nº 35, January 4, 2007, the National Telehealth Program in Brazil, with telehealth practices in the Brazilian Public Heal System.

COVID-19 brought a change in the uses of telemedicine in Brazil, being the approval and encouragement of the use of teleconsultation during the period of public emergency caused by the pandemic.

Until 2019, telemedicine was regulated under CFM Resolution 1,643/2002. Telemedicine is defined in the regulation as the "practice of medicine through the use of interactive methodologies of audiovisual and data communication, with the objective of health care, education and research" (article 1). This resolution does not bring any description of telemedicine modalities, and as for the procedural rules, it only indicates that the legal entities that provide telemedicine services must register in the regional councils.

On February 6, 2019, the CFM published CFM Resolution 2,227/2018, scheduled to go into effect 90 days after its publication, which allowed physicians to perform teleconsultations, tele-surgeries, telediagnosis, telemonitoring, tele-guidance, teleconsulting, among other forms of remote medical care. This resolution was cancelled 16 days after its publication, on February 22, 2019, being telemedicine continued to be subject to the terms of CFM Resolution 1,643/2002. It is worth noting that the reluctance to adopt telemedicine was configured on an argument that the practice would violate article 37 of the Code of Medical Ethics: "prescribe treatment and other procedures without direct examination of the patient".

With the COVID-19 pandemic in progress, and Brazil having recognized the situation of public health emergency,[4] in CFM Official Letter 1756/20, dated March 19, 2020, the CFM recognized the possibility of using telemedicine "on an exceptional basis and to combat the COVID-19 contagion", for: teleorientation, telemonitoring, and teleinterconsultation. Subsequently, on March 23, 2020, the Ministry of Health confirmed the position.[5]

On April 15, 2020, Federal Law nº 13,989/2020 was issued, which provides the use of telemedicine during the coronavirus crisis. The law does not provide further details about procedures and responsibilities. It does not provide any deep reflection involving care protocols and limits (or permissions) for the use of telemedicine in Brazil.

And what does this imply? On the one hand there are the principles of data protection, especially in the LGPD, in the sense of implement measures to ensure information security; however, on the other hand, from a technical point of view, there is no guideline referring which measures are valid. The market practice has recommended, like the Brazilian Society of Cardiology's Guidelines on Telemedicine in Cardiology – 2019[6], the requirements provided for the North American Law, the Health Insurance Portability and Accountability Act (HIPAA). HIPAA has represented a converging international industry standard for health data processing.

It should be noted that one of the advantages of adopting HIPAA, despite its normative force being restricted to the North American territory, is that the industry will now be evaluated and certified through a common normative.

Another standard to security information to be considered, on the other hand, at the national level, would be the one established by the "Sociedade Brasileira de Informática em Saúde" (SBIS – Brazilian Society of Health Informatics). CFM Resolution 1821/2007, about electronic medical records, stated that the Federal Council of Medicine and the SBIS, through a partnership, should issue a certificate of quality for computerized systems according to the Certification Manual for Electronic Health Record Systems. The partnership has ended, but the criteria could be used.

The central pending issue in the regulation is: which security mechanism standards should be used in health data, so as not to cause legal uncertainty for agents? Should agents adopt the international standard, taking into account the interoperability and ease evaluation of available products, or should agents

---

4 Under the Federal Law 13.979/20.

5 Ordinance Act Nº 467/2020.

6 Diretriz da Sociedade Brasileira de Cardiologia sobre Telemedicina na Cardiologia, 2019, https://cardiologiahmt.com.br/wp-content/uploads/2019/11/aop-diretriz-telemedicina-portugues.pdf [accessed: 22.04.2021].

create and/or use national solutions? In any case, the current regulations, in order to guarantee data security and medical confidentiality in the doctor-patient relationship, must be observed. However, the central key is the lack of interoperability among platforms, an issue already identified by EU.

Health data in the European Union

If in Brazil we have noticed these difficulties so far, in the European Union the issues were mapped in a study published on February 11, 2021, "Assessment of the EU Member States' rules on health data in the light of GDPR", by the European Commission[7] 15by the European Commission.[8]

The study assessed how EU Member States have implemented the GDPR regulations in their legislation for health data. The study was done in the context of creating a European Health Data Space, which is one of the European Commission's priorities for the period 2019–2025. The European Health Data Space aims to promote better exchange and access to different types of health data in a solid system of governance, valuing data quality and interoperability of the structure. The study highlighted the possible differences and identified the elements that could affect the international transfer and processing of health data in the EU for healthcare.

Despite the different approach scope between the EU, in the sense that each Member State can internalize the GDPR by changing some of its provisions, and Brazil, which is a single country that coexists with the regulatory problems identified above, the result of both is similar: the need for a cohesive regulation that provides interoperability between agents.

To examine the impact of the GDPR on the operation of digital health services, Member States were asked to indicate whether any specific legislation had been adopted in this context. Twelve Member States reported the existence of specific legislation.[9] The processing legal basis under GDPR will differ depending on the situation, with consent, followed by the provision of health care, representing the most common basis in the practical analysis of the study.

It is worth noting that both the GDPR and the LGPD, when establishing the legal basis of health care for the processing of sensitive data, limit it to health professionals, health services or health authorities, each regulatory diploma using its own language. Thus, it would not always be possible to consider

---

7 https://ec.europa.eu/health/ehealth/key_documents_en#anchor1 [accessed: 23.04.2021].

8 About the European Commission, https://ec.europa.eu/info/about-european-commission_en [accessed: 23.04.2021].

9 CZ, DE, EE, EL, FR, HR, LT, AT, PL, RO, SI, SK.

the health care as a general rule for the processing of health data – it will always depending on the case.

It is noteworthy that under the terms of the study, the German correspondent, in a pioneering way, mentioned a recently adopted regulation dealing with digital health in Germany.[10] Other countries, such as Austria, have guidance documents that are addressed to device manufacturers and provides interoperability standards, rather than enacting formal rules and legislation in this regard. England has addressed this problem in a similar way through the requirements for the NHS healthcare system.

The study broadly concluded that: (i) the current EU legal and regulatory frameworks are not aligned with recent innovations in digital health. Taking the area of telemedicine as an example, it was noted that there are currently serious interoperability problems between available solutions; (ii) moreover, Member States sometimes adopt or adapt specific international standards according to their own needs, which represents an additional barrier to interoperability; (iii) furthermore, incidents of data misuse by commercial parties, including those established outside the EU, raise awareness that compliance with data protection rules must be ensured. The challenge for Member States and the EU as a whole is therefore to find a balance between security and data sharing.

Final Considerations

First, the European Commission's initiative to create a specific working group to map the regulatory failures post-GDPR in order to achieve the European Health Data Space is noteworthy. The result of this research will allow the EU to act specifically on the failures and results found. It should also be noted that no study similar to the one carried out by the EU has been developed by Brazil.

Despite the advances that have occurred in Brazil to guarantee data protection, the regulation still presents flaws and points for clarification – for example, what technology guarantees full compliance with the security standards expected by Brazil? Would HIPAA be adopted? Any other national standard?

---

[10] "The procedure for the inclusion of a digital health application in the directory for digital health applications of the Federal Institute for Drugs and Medical Devices is initiated upon application by the manufacturer. Relying on § 5 I and § 6 of the Digital Health Application Ordinance, the manufacturer shall state in the application whether data processed via the digital health application can be exported by the insured person from the digital health application in an interoperable format and made available to the insured person for further use by 1 January 2021 at the latest. They shall also state whether the insured person can export relevant extracts of the health data processed via the digital health application for their care, in particular data on therapy courses, therapy planning, therapy results and data evaluations carried out, from the digital health application from 1 January 2021 at the latest."

The LGPD is in force without the corresponding penalties. Even if the possibility of civil liability in terms of compensation for damages arising from violation of the LGPD, there is the lapse of almost a year without any possibility of the supervise authority impose any kind of penalty. Second that the Brazilian legislation does not provide a definition or specific standards on health data. Third that there is an uncertain zone of conflict of competence among the regulatory bodies, including the professional councils. Fourth that the liability regime in the LGPD is unclear. These are issues only from the legal point of view of the law.

There is also no legal security about the establishment of telemedicine as a consolidated practice beyond the pandemic period. Neither there are standards or protocols for telehealth care. In addition, there are no procedural norms, technical aspects including information security, requirements for a consent form, liability regime involved, parameters for control and quality assessment of the services rendered in telemedicine as well.

Despite the different approach scope between the EU, in the sense that each Member State has the competence to internalize the GDPR by amending some of its provisions, and Brazil, which is a single country that coexists with the regulatory problems identified above, the result of both is similar: the need for a cohesive regulation with interoperability needs.

Bibliography

About the European Commission, https://ec.europa.eu/info/about-european-commission_en [accessed: 23.04.2021].

Diretriz da Sociedade Brasileira de Cardiologia sobre Telemedicina na Cardiologia, 2019, https://cardiologiahmt.com.br/wp-content/uploads/2019/11/aop-diretriz-telemedicina-portugues.pdf [accessed: 22.04.2021].

Gomes O., *Civil Liability*, Forense, Rio de Janeiro 2011.

Abstract

Health data processing in the context of telemedicine: an overview between Brazil and the European Union post pandemic COVID-19

The use of telemedicine had notably been developed in Brazil after the beginning of the public emergency period caused by the pandemic of COVID-19. With the new data protection law in force in Brazil, which is similar to the GDPR, health data are in the spotlight. The purpose of this article is to exam what measures Brazil has adopted to guarantee the data protection for health data in view of this scenario, taking the EU as a perspective

for comparison reasons. For the Brazilian analysis, not only the formal legislation was considered, but also the guidance of the Federal Council of Medicine, which is the competent authority to supervise and issue orders on the development of medicine in Brazil, including the telemedicine. The comparison with the EU was chosen due to the similar data protection regulation, since the LGPD presents similar provisions and regulations to those established in the GDPR, and because the European Commission has issued a study on February 11, 2021, assessing the implementation of the GDPR and the domestic regulations for health data in each of the EU countries. This article has found out Brazilian regulation still presents flaws and points for clarification, which are fundamental to guarantee the necessary legal security in operations.
Key words: telemedicine, LGPD, GDPR, Brazilian medicine, health data