InDi Institut für Internationale und Digitale Kommunikation
Institute for International and Digital Communication

Interdisziplinär. Angewandt. Innovativ. | Interdisciplinary. Applied. Innovative.

ZEITSCHRIFT FÜR INTERNATIONALE UND DIGITALE KOMMUNIKATION: NACHHALTIGKEITSPERSPEKTIVEN – JOURNAL OF INTERNATIONAL AND DIGITAL COMMUNICATION: SUSTAINABILITY PERSPECTIVES

Special issue: INTERNATIONAL VIRTUAL EXCHANGE COVID-19 - ETHICAL DILEMMAS AND HUMAN RIGHTS – EXPLORING INTERNATIONAL DIMENSIONS

Heft 1 (2022)
Issue 1 (2022)

Editors of the special issue:
Prof. Dr. Milena Valeva, Prof. Dr. Kathrin Nitschmann

Umwelt-Campus Birkenfeld | HOCHSCHULE TRIER

InDi Institut für Internationale & Digitale Kommunikation

THE USE OF TECHNOLOGICAL TOOLS IN THE FIGHT AGAINST COVID-19 & ITS IMPLICATIONS ON THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA AN APPROACH

Diego Zegarra Valdivia PhD. [**]
Senior Lecturer in Administrative Law
Pontifical Catholic University of Peru

Abstract: This paper analyzes some of the assumptions in which the varied use of technologies to confront the spread of the COVID-19 pandemic and protect people's health has impacted on the fundamental right to the protection of personal data; to do so, it starts from the premise that the use of these technologies cannot mean an affectation to the referred fundamental right, much less an indiscriminate treatment of such data without any minimum control whatsoever.

Keywords: Fundamental Right - Personal data protection - Pandemic - COVID-19 - Consent - Public Health -Technology - Public Health

Summary: I. Introduction. II. The Bases of Legitimacy of Health Data Processing. 1. Consent in the Processing of Health Data. 2. Purpose, Proportionality, and Data Minimization. 3. Security. 4. Quality or time-limited Storage. III. The Use of technological Tools based on the Processing of Personal Data to fight the COVID-19 Pandemic. 1. Information and Diagnosis of the Virus. 2. Geolocation and Tracking of infected People. 3. Mass Temperature Measurement in Public Spaces. IV. Conclusion.

I. Introduction

The COVID-19 pandemic has led almost all countries worldwide to progressively adopt various types of measures to contain its spread, protect public health and people's lives (Gómez-Córdoba et al., 2020, p. 273). These measures include mandatory social isolation, social distancing, capacity control, the use of technological tools for data processing and mitigation of contagion, the establishment of information channels on

* This research is part of the activities of the Research Line on Personal Data Protection and Transparency of the Research Group on Administrative Law GIDA and its elaboration counted with the collaboration of Camila Chinchay, Ángela Casafranca, Christian Hernández, Alexandra Olivera, Piero Curi and Camila Atencio.

** D. in Law from the University of Alicante, Master in Telecommunications and Information Technology Law from the University Carlos III of Madrid, Director of the Master in Administrative Law and the Second Specialization Program in Administrative Law at the Pontificia Universidad Católica del Perú. Head of the Academic Office of Internationalization and Coordinator of the Administrative Law Area at the Law School of the Pontificia Universidad Católica del Perú.

COVID-19, geolocation of infected people, mobility studies, contact tracing and registration, control, and measurement of body temperature, among others.

All these actions in one way or another have limited fundamental rights and freedoms such as privacy, protection of personal data, freedom of movement, freedom of expression, freedom of assembly, among other rights. Of those mentioned, the fundamental right to the protection of personal data is important for the purposes of this paper, due to the type of information collected and required for the implementation of epidemiological surveillance systems and control of the spread of the disease (Gómez-Córdoba et al. , 2020, p. 273).

Measures to mitigate COVID-19 necessarily involve the processing of different personal data, whereby appropriate and lawful processing must be ensured. While the severity of the current health crisis allows for the use of emergency powers in response to major threats - as noted by a group of UN human rights experts on 16 March 2020 - it is imperative that the response to be implemented by States in the face of COVID-19 is proportionate, necessary, and non-discriminatory (UN, 2020).

It should be noted then, that under no circumstances does the declaration of health emergency assumed globally by countries imply, either expressly or tacitly, the suspension of the fundamental right to the protection of personal data, it only implies adopting certain measures that bring with them the limitation and not the suspension in the exercise of rights and freedoms (Piñar, 2020). However, as Arenas (2020) argues, the important thing is that these limitations must comply with a series of requirements and offer a series of guarantees and responsibilities in case of non-compliance: they must be necessary, appropriate, and proportional in a democratic society (p. 10).

It is a different matter whether it is necessary to adapt this fundamental right to, as the Spanish Data Protection Agency (hereinafter, AEPD) has stated, "(...) legitimately permit the processing of personal data in situations, such as the present one, in which there is a health emergency of general scope" (2020, p.1). The latter has been reiterated by the European Committee for the Protection of Personal Data, having emphasized that respect for the privacy of individuals does not constitute a stumbling block in making decisions that involve containing the current pandemic, when we are talking about sensitive data such as those relating to the health of individuals (EDPB, 2020, p. 1).

In the months that this pandemic has been going on, voices have arisen to express whether "privacy will be one of the victims of COVID-19" (Renda, 2020), expressions such as "to death by data protection" (Martínez, 2020) have been coined, or statements regarding whether the concessions and restrictions on surveillance, tracing, tracing and security of citizenship could become permanent (Calzada cited by Recuero Linares, 2020, p. 141), which makes manifest the uncertainty regarding the guarantees that legal systems have established for the exercise of this fundamental right and the rights linked to it. Therefore authors such as Andreu (2020) consider problematic the application of the regulations "in the use of technological solutions for the fight against the pandemic,

which has led to restrictive statements about their use and great confusion about their efficacy and safety" (p. 851).

Indeed, these innovations have generated new concerns worldwide about the inappropriate use of certain applications that affect the fundamental right to the protection of personal data and the privacy of citizens, which has led to a tension between the right to collective health and individual rights. And the fact is that, unfortunately,

These strategies are not always contextualized within a robust personal data protection regime, nor within legal instruments that guarantee that in their development and implementation the rights of individuals are protected, that only truly necessary data are obtained, that the impact on human health that justifies the restrictions of freedoms is evaluated, or that the information obtained will not be used in the long term for other state or private purposes (Gómez-Córdoba et al., 2020, pp. 274-275).

It is for these considerations that this paper aims to analyze that, although the context of COVID-19 requires rapid measures to address its expansion and mitigate its impacts, relying on technology as a suitable and necessary means for this purpose by accessing sensitive data such as the health of individuals or personal data and their geolocation, there is great concern about the proper treatment and use of these personal data collected in these circumstances because the use of these technologies can not mean an affectation of the fundamental right to the protection of personal data, much less a treatment of personal data, there is a great concern for the proper treatment and use of these personal data collected in these circumstances because the use of these technologies can not mean an affectation of the fundamental right to the protection of personal data, much less an indiscriminate treatment of such data without any minimum control.

II. The Bases of Legitimacy of Health Data Processing

The processing of personal data in these health emergency situations continues to be carried out in accordance with the regulations on personal data protection, so that all its principles are applied, including the processing of personal data with lawfulness, loyalty and transparency, purpose limitation, the principle of accuracy and data minimization (AEPD, 2020, pp. 6-7). Therefore, without reaching the alarmist excess of the aforementioned expressions, under the premise that the legal systems legitimize the processing of personal data that are essential to fight against the global pandemic of COVID-19, this article identifies the possible risks and affectations to the fundamental right to the protection of personal data derived from the implementation by States and individuals of technological tools in order to control the spread of the virus, protect public health and the life of people, and formulates some reflections on the scope of the same in the guarantee of the aforementioned fundamental right.

The protection of personal data is a fundamental right recognized in various international texts, in comparative legislation, as well as in the Peruvian legal system.

At the international level, as Razquin points out, the protection of personal data is provided for in:

Art. 12 of the Universal Declaration of Human Rights of 1948 and Art. 17 of the International Covenant on Civil and Political Rights of 1966, which refer to the protection of privacy and intimacy. Also within the Council of Europe, Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 establishes the principle of protection of privacy; Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 guarantees the protection of data against automated processing; and also the Council of Europe Convention on Access to Public Documents of 2009 includes as one of the limits of the right of access to documents the protection of privacy (Article 3.1.f). The Treaties of the European Union also protect the protection of personal data (art. 16 TFEU and art. 39 TEU). And the Charter of Fundamental Rights of the European Union regulates the right to the protection of personal data (Art. 8). (2019, p. 142).

Likewise, at the European level, in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter, GDPR), regulates the processing of personal data and the free movement of such data in a reality associated with the new digital society, having collected for it in its Article 5 the basic principles that should govern them, such as lawfulness (whose scope has been developed in Article 6 of the RGPD), fairness and transparency; purpose limitation; data minimization; accuracy; limitation of the retention period; and, integrity and confidentiality.

For its part, in the Peruvian legal system, the recognition of the protection of personal data as a fundamental right has been included in Article 2, paragraph 6 of the Political Constitution of Peru, which stipulates the right of every person to ensure that computer services, whether computerized or not, public, or private, do not provide information that affects personal and family privacy.

The normative development of the aforementioned constitutional precept has been carried out in Law No. 29733 - Personal Data Protection Law (hereinafter, LPDP), enacted in 2011 and in full force since 2013, and in its Regulations approved by Supreme Decree No. 003-2013-JUS (hereinafter, RLPDP). Through this regulation seeks to guarantee the fundamental right of the holders of personal data, that is, the ability of the same to control their treatment in the field of Public Administration as that which occurs in the private sector.

During this pandemic, the collection and processing of personal data related to health is constant. These data are considered as a special category in the personal data protection regulations, whose main characteristic is their sensitive nature. These are data whose processing may involve a greater risk of infringement of the rights and freedoms of the data subject and therefore are worthy of special protection because they can significantly affect the individual.

Health data consists of those information "that refer to past, present or future health in healthy or sick people, with diseases of a physical or psychological nature, and includes addiction to alcohol and drugs" (Cristea, 2018, p. 46). Personal data referring to health, contain, as Cristea points out, information about people that makes it possible to know the ailments or diseases they have suffered, suffer, or may even suffer (2018, p. 46). Solernou further refers that the European Group on Ethics in Science and New Technologies considers that personal health data includes information relating not only to diseases, but also to interventions, prescribed medicines, diagnoses, etc.; as well as administrative health data referring to registration, and admissions, insurance, etc. (2006, pp. 51-52).

It is, in short, personal data that are part of the most intimate sphere of the person, which may be revealing critical situations related to certain diseases, to the application of assisted reproduction techniques or related to genetic information, whose potential violator of personal privacy no one dares to doubt (Piñar, quoted by Cristea, 2018, p. 46).

It is because of the scope of the definition of health data that it is essential to analyze the framework of guarantees of the principles of legality, consent, purpose, proportionality, quality, security, availability of the resource, and adequate level of protection, contained in the LPDP (Title I) and in the RLPDP (Title II) since they delimit the processing of personal data, have binding force, practical application and define whether or not a data processing is being carried out in a fair, lawful, transparent and adequate manner. However, in the health emergency situation, the previous principles contained in the Peruvian legislation, to which it is reasonable to add - due to their connection - those that have been included in the European GDPR, are difficult to comply with for the processing of health data in a digital environment. Therefore,

There is an urgent need to clarify and specify the application of data protection principles to new technologies, in order to ensure real and effective protection of personal data, whatever the technology used to process these data, and that data controllers are fully aware of the implications of new technologies on the protection of personal data (Cristea, 2018, p. 224).

It is then necessary to identify the scope of the aforementioned principles and the effects derived from the implementation of technological tools that involve the processing of health data in the understanding that it is a series of material rules designed to develop and ensure the achievement of the purposes of the personal data protection regulations.

1. Consent in the Processing of Health Data

The principle of consent implies that third parties may access personal data, provided that there is free, express, unambiguous and informed consent from the owner. This

principle is contained in article 5[1] of the LPDP and articles 7, 11, 12 and 14 of the RLPDP.

In accordance with what is regulated in the LPDP, Article 7[2] of the RLPD, provides that the data subject's consent implies any free, specific, informed and unambiguous expression of will by which the data subject accepts, either by a statement or a clear affirmative action, the processing of personal data concerning him/her. Thus, as Arias (2016. p. 122) argues, consent has its own way of being granted:

- by a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject's free, specific and unambiguous wish to consent to the processing of personal data concerning him/her. It may be a written statement, including by electronic means or a verbal statement, if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not necessarily disruptive to the use of the service for which it is provided;
- for all processing activities carried out for the same purpose(s), i.e. where the processing has several purposes, consent must be given for each of them;
- by a means which enables the controller to be able to demonstrate that the data subject has consented to the processing operation.

Likewise, the LPDP has provided in article 14[3] the cases in which the processing of personal data without consent is legitimate. Thus, paragraph 6 of the previously mentioned article provides that the consent of the owner of the personal data is not required, for the purposes of its processing, "when there are reasons of public interest

---

1 Law No. 29733, Personal Data Protection Law, „Principle of consent For personal data tob e processed, the consent oft he data subject must be obtained“.

2 Supreme Decree No. 003-2013-JUS, Regulation of Law 29733.
„Article 7 – Principle of consent: In accordance with the principle of consent, the processing of personal data is lawful when the owner of the personal data has given his free, prior, express, informed and unequivocal consent. Consent formulas in which consent is not directly expressed, such as those in which it is required to presume or assume the existence of a will that has not been expressed, are not admissible. Even the consent given with other declarations must be expressed expressly and clearly“.

3 Law No. 29733, Personal Data Protection Law
"Article 14. Limitations on consent to the processing of personal data
The consent of the holder of personal data is not required, for the purposes of its processing, in the following cases: (...)
6. When it concerns personal data relating to health and it is necessary, in circumstances of risk, for the prevention, diagnosis and medical or surgical treatment of the holder, provided that such treatment is carried out in health establishments or by professionals in health sciences, observing professional secrecy; or when there are reasons of public interest provided by law or when they must be treated for reasons of public health, both reasons must be qualified as such by the Ministry of Health; or for the performance of epidemiological or similar studies, provided that appropriate dissociation procedures are applied. (...)".

provided by law or when they must be processed for reasons of public health, both reasons must be qualified as such by the Ministry of Health".

The scope of this rule has been explained in Advisory Opinion No. 07-2019-JUS/DGTAIPD-DPDP of the National Authority for the Protection of Personal Data, according to which, the exception regulated by paragraph 6 of article 14 of the Law on the Protection of Personal Data "refers to specific situations that involve a circumstance of risk, such as an epidemic, in which the life or health of the owner of the personal data and of persons close to him or her is endangered" (2019). Thus, when there are reasons of public interest or declared public health, such as the Health Emergency in force in Peru, the processing of personal data is allowed without requiring the consent of the owner of the personal data in order to take preventive measures against possible contagions. A similar provision has been foreseen in paragraph i of Article 9[4] of the European GDPR: "sensitive data may be processed for rea-sons of public interest in the area of public health, such as protecting against threats to public health or ensuring medical device quality" (Scheibner et al., 2020, p. 12).

Therefore, given the need to have information for the proper management of the pandemic, it is admissible to process personal data of a general nature and those relating to health without the consent of the data subjects. However, this processing must be justified, necessary, proportional, reasonable and effective as a measure to contain the spread, and the security of the data processing must be guaranteed.

It should also be borne in mind that the processing of health data for the purposes of prevention or medical diagnosis, for the provision of health care and for the management of health services is legitimate, provided that the processing is carried out by persons subject to the duty of confidentiality (Solernou, 2006, p. 56). "This processing includes the collection, storage and communication of data and is lawful provided that it pursues these purposes and is carried out by persons bound by professional secrecy" (Solernou, 2006, p. 56).

With regard to the initiatives from the States and the private sector that have involved the implementation of technical solutions and mobile applications for the collection of health data in order to improve the operational efficiency of health services, as well as to achieve better care and accessibility by citizens, they are not within the exception mentioned above since we are dealing with functionalities that are made available to citizens and their use is voluntary and requires express consent.

---

4 Regulation (EU) 2016/679
"Article 9. Processing of special categories of personal data (...)
2. Paragraph 1 shall not apply where one of the following circumstances applies: (...)
(i) processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or to ensure high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law providing for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular professional secrecy. (...)".

The use of applications ("app") that allow the owner of the personal data to self-assess based on the medical symptoms he/she communicates, the probability of being infected with COVID-19, to receive information, advice and recommendations, or to enable geolocation to verify that he/she is where he/she claims to be, must be entirely voluntary, so that any person who wants to submit to them will have to give their express consent, where the controller will be the state health authority or the private company that makes it available (Rodriguez, 2020, p. 143).

2. Purpose, Proportionality, and Data Minimization

The processing of health data that are collected must be exclusively limited to the intended purpose, without extending such processing to any other personal data not strictly necessary for that purpose, or that may be confused convenience with necessity, because the fundamental right to data protection must continue to apply without prejudice to the emergency situations established in the regulations for the protection of essential public health interests (Piñar, 2020).

According to the latter, the collection of personal data should be minimal for the achievement of public health objectives, being in line with the principle of proportionality, whose purpose is "to avoid collecting information that is not reasonably relevant to fulfill the purpose of the processing, which implies a limitation for any form of collection that is not justified" (Zegarra 2014, p. 631).

The guarantee that the processing of personal data is determined, explicit, lawful and that it will not be incompatible with the purposes for which it was collected; as well as that the processing of personal data is adequate, relevant, and not excessive, all for the purpose of making health prevention measures effective, are regulated in articles 6[5] and 7[6] of the LPDP, respectively. In accordance with the aforementioned rules, it is necessary to verify the compliance of the purpose and relevance of the personal data requested with the regulations that the health authorities have approved whose purpose is to address COVID-19 and reduce its spread.

---

5 Law No. 29733, Personal Data Protection Law
"Article 6. Principle of finality
Personal data must be collected for a specific, explicit and lawful purpose. The processing of personal data must not be extended to any purpose other than the one unequivocally established as such at the time of collection, excluding cases of activities of historical, statistical or scientific value when a dissociation or anonymisation procedure is used".

6 Law No. 29733, Personal Data Protection Law
Principle of proportionality
Any processing of personal data must be adequate, relevant and not excessive to the purpose for which the data were collected".

Linked to the principle of proportionality of the Peruvian legislation is the principle of data minimization, contained in Article 5[7] of the European GDPR, according to which personal data can only be collected strictly necessary for the processing and at the time they are going to be processed, not to use them later; also, the request for personal data from their owners must be fully justified, depending on the purpose pursued by such processing (Puyol, 2017, p. 138).

Faced with the new challenges in times of pandemics, the principles that underpin the processing of personal data must be reinterpreted to have a regulatory framework that provides legal certainty, protects the rights of individuals and generates trust in society (Gómez-Córdova et al., 2020, p. 285). Thus, for example, the principle of purpose in the processing of personal data is linked to the ethical recommendations of the WHO in the COVID-19 pandemic referring to (i) the restriction of its use; (ii) proportionality in the collection of data; and (iii) the minimum collection of data for the achievement of public health objectives (Gómez-Córdova et al., 2020, p. 286).

It is necessary to note that there is a tendency to collect a lot of health data and the use of information technology contributes to this, thus affecting the efficiency of health care provision (Souleron, 2006, p. 57). "The system must ensure that health workers have necessary and relevant information when exercising their functions and this involves deciding and, if possible, questioning what data is entered into the system and in what form." (Souleron, 2006, p. 57).

From what has been expressed, it is clear that, although these considerations are prior to the health emergency generated by the COVID-19, they point to warn that the use of information technologies in the processing of health data may result in the non-observance of the principles of purpose, proportionality and data minimization, This has a significant impact in the event of access to personal data by unauthorized third parties, since it may result in processing for unauthorized uses or processing that limits the exercise of the rights of the owner of the personal data, hence the importance of establishing mechanisms to ensure compliance with the aforementioned principles.

3. Security

The principle of security implies that any personal data processing mechanism adopted must guarantee the security of personal data to prevent any loss, deviation or adulteration of the personal data obtained. In the specific case of health data, the security measures to be implemented are of high level, attending to the nature of the

[7] Regulation (EU) 2016/679
"Article 5. Principles relating to treatment
1. The personal data will be: (...)
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation"). (...)".

referred data and according to the greater need to ensure the confidentiality and integrity of such information when it is treated (Cristea, 2018, p. 108).

Peruvian law has included these terms. Thus, in accordance with article 9[8] of the LPDP and article 10[9] of the RLPD, the principle of security guarantees that the owner of the personal data bank and the person in charge of its processing must adopt technical, organizational and legal measures necessary to safeguard the security of personal data, avoiding any processing contrary to the Law or the Regulation, including adulteration, loss, diversion of information, intentional or not, whether the risks come from human action or from the technical means used.

For its part, Article 4.12[10] of the European GDPR states that a breach of security of personal data means any breach of security resulting in the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed. Furthermore, Article 5[11] of the GDPR ensures adequate security of personal data, which implies protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage by appropriate technical or organizational measures ('integrity and confidentiality').

The guarantee of the principle of security is directly linked to the right to confidentiality of personal data. However, the availability of measures that aim to guarantee the right

---

8 Law No. 29733, Personal Data Protection Law
"Article 9. Principle of security
The owner of the personal data bank and the processor must take the necessary technical, organisational and legal measures to ensure the security of personal data. The security measures must be appropriate and commensurate with the processing to be carried out and the category of personal data concerned.".

9 Supreme Decree No. 003-2013-JUS, Regulation of Law 29733
"Article 10.- Principle of security
In accordance with the principle of security, in the processing of personal data, the necessary security measures must be adopted in order to avoid any processing contrary to the Law or to these regulations, including adulteration, loss, diversion of information, whether intentional or not, whether the risks arise from human action or from the technical means used".

10 Regulation (EU) 2016/679
"Article 4. Definitions (...)
breach of security of personal data" means any breach of security resulting in the accidental or lawful destruction, loss or alteration of, or unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed; (...)".

11 Regulation (EU) 2016/679
"Article 5. Principles relating to treatment
1. The data shall be: (...)
(f) processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical or organisational measures ("integrity and confidentiality")".

to health and that make it possible to provide timely and accurate information, improving access to health data fusing information technologies, does not necessarily guarantee the security of such data.

It is necessary to note that the patient's trust in confidentiality depends on the security of the technical apparatus and the transparency of the treatment of personal health data, both of physicians and non-physicians involved in the operations and processes. (Almada & Maranhão, 2021). Therefore, access should not be indiscriminate, even when it is based on scientific reasons, so mechanisms should be implemented to avoid affecting the security of health data, i.e., its integrity and confidentiality.

4. Quality or time-limited Storage

The processing of personal data collected within the framework of the exemption from the obligation of consent by health authorities or by private companies, within the framework of the exemption from the obligation of consent, should be limited, as for any processing, to the duration of the health emergency situation, thus ensuring that the information obtained will not be used in the long term for other state or private purposes.

This rule has been included in Article 8[12] of the PDPL, which provides that personal data must be kept in a manner that ensures their security and only for the time necessary to fulfil the purpose of the processing. Likewise, article 28[13] of the LPDP establishes the obligation of the data controller, when the data are no longer relevant, necessary, and adequate for the established purpose, to delete or anonymize them or must apply a mechanism of dissociation or pseudonymization with code, the data will remain active, but without being able to easily identify the owner of the data, safeguarding his right to the protection of personal data.

The European GDPR includes a provision whose content is in harmony with the aforementioned rules of the Peruvian DPL.

---

12 Law No. 29733, Personal Data Protection Law
"Article 8. Principle of quality
The personal data to be processed must be true, accurate and, as far as possible, up to date, necessary, relevant and adequate in relation to the purpose for which they were collected. They must be kept in a form which ensures their security and only for the time necessary to fulfil the purpose of the processing".

13 *Law No. 29733, Personal Data Protection Law*
"Article 28. (...)
7. Delete the personal data being processed when they are no longer necessary or relevant to the purpose for which they were collected or when the time limit for their processing has expired, unless anonymisation or disassociation procedure is used. (...)".

In its article 5[14], the GDPR provides that personal data must be kept in a form that allows the identification of data subjects for no longer than is necessary for the purposes of the processing of the personal data ("limitation of the retention period").

After that time they can only be kept for longer periods for the purposes of archiving in the public interest, scientific or historical research purposes or statistical purposes, being sometimes necessary, in order to safeguard the principle of minimization, to proceed to the pseudonymization of the data (RGPD art. 89.1), and without prejudice to the application of appropriate organizational techniques imposed by the RGPD to protect the rights of the data subject (López, L.F., 2016, p. 61).

III. The Use of technological Tools based on the Processing of Personal Data to fight the Covid-19 Pandemic: Identification of some Risks and Effects on the Fundamental Right to the Protection of Personal Data

With the declaration of the pandemic by COVID-19, several nations around the world have implemented numerous initiatives aimed at mitigating the harmful effects of the virus through the development of technological tools based on the processing of health data. The latent threat to human life posed by COVID-19 makes it necessary to contain it through the correct management of personal data and suitable means to this end.

Therefore, in recent months various governments and private companies have implemented digital strategies that complement the epidemiological surveillance tools for case detection, contact tracing, diagnosis of the disease, documentation of places where people have been, determination of sites and times of greatest influx, in order to implement measures to limit contagion. In addition, they have been used to communicate and educate citizens or provide health care through telepresence (Gómez-Córdoba et al. , 2020, p. 274). This has been recognized at the international level in Resolution No. 1/2020 of the Inter-American Court of Human Rights, entitled "Pandemic and Human Rights in the Americas":

Regarding the containment measures to confront and prevent the effects of the pandemic, the IACHR has observed that some rights have been suspended and restricted, and in other cases "states of emergency," "states of exception," "states of catastrophe due to public calamity," or "sanitary emergencies" have been declared

[14] Regulation (EU) 2016/679
"Article 5. Principles relating to treatment
The data will be: (...)
(e) kept in a form which permits identification of ¬data subjects for no longer than is necessary for the purposes for which the ¬personal data are processed¬; personal data may ¬be kept for longer periods provided that they are processed exclusively for ¬archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), without prejudice to the application of appropriate technical and organisational measures imposed by this ¬Regulation in order to protect the rights and freedoms of the data subject ('limitation of the retention period')".

through presidential decrees and regulations of various legal natures in order to protect public health and prevent an increase in contagion. Likewise, measures of different nature have been established that restrict the rights of freedom of expression, the right of access to public information, personal liberty, the inviolability of the home, the right to private property; and the use of surveillance technology has been used to track the spread of the coronavirus, and the massive storage of data. (IACHR, 2020, p.4).

The so-called surveillance technology has materialized in applications whose main intention is to inform about the virus and provide a diagnosis based on the data entered in the application and identify infected individuals, foci of contagion and allow the tracking and tracing of the contagion. Likewise, technological tools have been implemented that have allowed massive temperature measurements in public spaces.

There is no doubt that the implementation of new technologies based on the processing of personal data, together with the use of data analytics and Artificial Intelligence techniques, bring significant benefits and represent an important opportunity to stop the spread of COVID-19, as they improve the forecasting and decision-making capacity of health authorities, contribute to strengthening the effectiveness of social distancing measures, thereby significantly reducing the spread of the pandemic and minimizing the cost of human lives (Domínguez, 2020 p. 610).

However, as previously noted, these strategies are not always configured within a robust personal data protection legal regime that duly guarantees the protection of personal data and its principles, which justifies identifying, for their prevention, the risks that are generated when using technological tools that process personal data and the possible affectations to the fundamental right to the protection of personal data, especially when their use has made the methods of collecting personal data increasingly abundant, complicated and more difficult to detect (Cristea, 2018, p. 226).

This context raises the need to analyze those issues that will make it possible to achieve the difficult balance between the promotion of technological instruments that contribute to controlling the effects of COVID-19 by increasing the resources made available to the health authorities and the safeguarding of the fundamental right to the protection of personal data.

1. Information and Diagnosis of the Virus

Having information channels that are permanently updated about COVID-19, its symptoms, prevention measures and diagnosis is a matter of interest for anyone who has even the slightest symptom or seeks information that needs to be shared in their family environment.

Faced with the collapse of the telephone service for consultations, States, private companies, supranational organizations developed apps, websites, chatbots, Telegram channels, among others, so that citizens can obtain accurate and official information or perform self-assessments in a simple way, without having to make a phone call or go

to the emergency of a public or private health center (Cascón-Katchadurian, 2020, p. 4).

As for the self-assessment applications, they provide recommendations on how to act according to the symptoms, including contacting users for coronavirus testing or monitoring the evolution of the disease (Cascón-Katchadurian, 2020, p. 4). All these data are also used to make an approximate representation of the possible level of immunity of the population (Cascón-Katchadurian, 2020, p. 4).

In Spain, the General Secretariat for Digital Administration, under the Secretary of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation, developed the mobile application Radar COVID. By downloading it, users of this app receive a notification if, in the event that in the fourteen days prior to the download, they have been exposed to an epidemiological contact with another user who has declared in the application to have given a positive result in the COVID-19 test, after accreditation by the corresponding health authorities (Domínguez, 2020).

In South Korea, the app Self-quarantine safety protection was developed with the aim of preventing the uncontrolled spread of the disease and the collapse of hospitals, for which it records the data of users and their answers to questions about the state of health and with the same doctors offer a remote diagnosis which helps to decongest the phones (Cascón-Katchadurian, 2020, p. 5). "In this way a massive diagnosis is achieved and with this data it is decided who should be tested" (Ruiz, 2020 cited in Cascón-Katchadurian, 2020, p. 5).

In the Peruvian case, the app that has taken charge of providing updated information on the areas of contagion and providing citizens with a prognosis of their possible status as carriers of COVID-19 was called "Peru in your hands", which "offers the option "Map of affected areas" (....) to access a map near it where the incidence of infection is marked....) to access a map of the vicinity where the incidence of contagion is marked; there is also the option "Triage" (...) through which, according to the symptoms that are recorded, you can determine whether or not you are a possible carrier of the virus". (Vásquez, 2020, p. 158).

With regard to the risks or possible effects on the right to the protection of personal data that may arise from this type of apps, those linked to the principle of consent of individuals should be considered, since there is a danger that both the data entered by individuals to receive informative updates about the virus and the data entered to generate a self-diagnosis of the app are used for a purpose other than that which the user believed and consented to.

The analysis is based on the consideration that when a user provides their identification and health data to be informed and/or self-assessed by the application, their consent will revolve around the specific purpose of the service; therefore, the data controller

managing the app could not use the data for a purpose other than diagnosing the virus with the user's data.

Regarding the applications that are able to perform a self-diagnosis, there are those that achieve it based on the voice recording of people. In Spain, for example, the company Biometric Vox is developing an app that will be able to detect a COVID-19 contagion index, using artificial intelligence. This system would make it possible to analyse - remotely, without physical contact and in real time - the state of the speaking apparatus and, as a result, be able to provide an index of contagion and serve the health authorities as a complementary aid for the control of the spread and any other data management (Biometric Vox, 2020, para. 4).

In Brazil, SPIRA and SoundCov are two applications in which users make a recording of their voice that is then analyzed through machine learning algorithms resulting in a diagnosis of COVID-19 (Almada & Maranhão, 2021, pp. 1-2).

> The SPIRA project, currently under development at the University of Sao paulo, seeks to detect severe respiratory insufficiency associated with the SARS-COV-2 virus, to indicate whether the user of the app must seek hospitalization. To obtain this diagnosis, the SPIRA app records the patient's reading of a few pre-defined sentences. These recordings are analyse by a machine learning model trained to distinguish the voices of healthy persons from those of pleople afflicted with respiratory insufficiencies (Almada & Maranhão, 2021, p. 2).
>
> [The SPIRA project, currently under development at the University of Sao Paulo, aims to detect severe respiratory failure associated with the SARS-COV-2 virus, to indicate whether the user of the application should be hospitalized. To obtain this diagnosis, the SPIRA application records the patient's reading of predefined phrases. These recordings are analyzed by a machine learning model trained to distinguish the voices of healthy people from those of people affected by respiratory failure].
>
> SoundCov, an app developed by Fiocruz, Intel, and Instituto Butantan, trains a machine learning system to distinguish between the coughing sounds of a Covid-19-positive person and those of healthy people and people afflicted by other respiratory illnesses, such as pneumonia or tuberculosis. The application then combines the analysis of the coughing sounds with additional information about epidemiological variables and patient's health history, thus producing a final diagnosis (Almada & Maranhão, 2021, p. 2).
>
> [SoundCov, an application developed by Fiocruz, Intel and the Butantan Institute, trains a machine learning system to distinguish between the cough sounds of a person who tests positive for Covid-19 and those of healthy people and people affected by other respiratory diseases, such as pneumonia or tuberculosis. The application then combines the analysis of cough sounds with additional information

> on epidemiological variables and the patient's health history, resulting in a final diagnosis].

With this type of technology, the principle of consent may be violated, since consent must be obtained by providing health data subjects with all the information about the form and duration of the processing, so that if this does not occur, the consent is considered invalid (Almada & Maranhão, 2021, p. 7). Linked to the latter, it should be noted that applications based on machine learning systems are notoriously opaque to external observers, which poses additional difficulties to the task of providing users with the information they need to give informed consent (Almada & Maranhão, 2021, p. 7).

Furthermore it identifies the possibility of transgressing the principle of purpose applicable to the processing of personal data and, therefore, affecting the owner of such data, since

> Storing voice data, makes it possible for unauthorized entities to use the data to identify individuals, maliciously gain access to systems that implement voice recognition, or simply process data and build voice artifacts that could be used to impersonate individuals creating scenarios that are problematic (Alva, 2020, p. 171).

Another situation that can generate risks and impacts is the one that occurs when those responsible for the apps keep health data indefinitely. The latter is directly related to the principle of quality and implies that those responsible for the processing of health data must ensure that the information obtained will not be used in the long term for other state or private purposes but must be limited to the duration of the pandemic.

Thus, the exposure that the owner of the health data who accesses this type of app may have to the use of their information being used for different purposes is high, so it is essential to identify the company that makes the application available and review their privacy policies, prior to entering personal data in order to obtain information and / or perform a self-diagnosis.

2. Geolocation and Tracking of infected People

At this point, it is necessary to make a preliminary conceptual clarification because the use of mobile phones to help control the pandemic, there are two main possibilities: one based on geopositioning (or tracking) and another based on the automated tracking of contacts (or tracing) (Buchland, 2020).

According to the distinction, while the actual tracking uses the app which is installed on a mobile phone saving the location of the person constantly, tracing seeks to carry out an automated monitoring of contacts, which involves direct communication between a person's mobile phone and all those people with whom he or she wants to be in close contact (Buchland, 2020).

The truth is that, as we will see below, neither the tools focused on tracking, nor the apps aimed at tracing are free from the great dangers that arise in terms of personal data.

a. Geopositioning (Tracking)

Faced with the advance of COVID-19, the States have implemented technological initiatives aimed at knowing the movements of the population so that through their study they have patterns of mobility of people around a city, region or country, in order to record the location of infected people (or not infected, so that they do not avoid confinement) to assist them if necessary. Therefore, the knowledge of this data is beneficial for the Administration entities in charge of health, security and infrastructure, at the time of articulating and dimensioning the actions that mitigate the virus, so that they can do it in the most appropriate way (AEPD, 2020a, p. 5).

The tool that allows to use this data is the geolocation or geopositioning. Geopositioning uses an app (application on the smartphone) that uses the Global Position System (GPS). What should be considered is that this type of tool has some practical problems, such as the lack of accuracy in geolocation (especially indoors), or that mobile phones only report that users have been close to a person, among others. (Buchland, 2020).

However, although the limitations that accompany technology are well known, the truth is that the context of the pandemic has involved a proliferation of technological solutions that have been intended to support the fight against the pandemic (Andreu, 2020, p. 851). This is the case of the HaMagen app, which has been an example of how tracking can be an interesting tool for a government to undertake efficient actions for its population. The functionalities of this application have been explained by the Ministry of Health of Israel:

> HAMAGEN is an app that allows the identification of contacts between diagnosed patients and people who came in contact with them in the 14 days prior to the patient's diagnosis of the disease.
>
> Cross-referencing your location data with the corona patients' lo-cation is done on your device and as soon as a match is identified, you will be directed to a link to the Ministry of Health to let you know what steps to take and to report the match to The Ministry (Israel National Cyber Directorate, 2020, p. 1).
>
> [HAMAGEN is an app that allows you to identify contacts between diagnosed patients and the people who were in contact with them in the 14 days prior to the diagnosis of the patient's disease. The cross-referencing of your (the user's) location data with the location of Corona patients is performed on your device and, as soon as a match is identified, you will be directed to a link to the Ministry of Health to inform you of the steps to take and to report the match to the Ministry].

Geolocation through mobile devices can operate in two ways: by telecommunications operators and from social networks[15]. However, neither of these forms is devoid of risk.

In the case of geolocation carried out through mobile phones by telecommunications operators, mobile phone operators are "providing anonymized information on the location of their users in the telephone cells that define their antennas" (AEPD, 2020a, p. 4). The risk is that, in case of incomplete anonymization, lax outsourcing or a cyber-attack, the users´ information such as location and other shared information may be available to a non-authorized third party.

The geolocation of mobile phones from social networks is a technique used before the pandemic due to the fact that the IP addresses of users can be traced by the administrators of the websites. This is commonly used for advertising purposes. The shared information, in this case the location, can be of use to health authorities but only if it is in accordance with a previously defined purpose and is applied to their prevention and control strategies (AEPD, 2020a, p. 6).

Geolocation can provide some trends and statistics of contagion to government operators so that there is more action on their part in different areas. Geopositioning today can also be an excuse for abuses against the fundamental right of the protection of personal data, there are even those who consider that "the unprecedented expansion of state surveillance and control through digital technologies to monitor the possible transmission of the virus implies a significant regression in human rights that will be difficult to reverse in the post-pandemic scenario" (Bizberge and Segura, 2020, p. 71).

b. Contact Tracing and Tracking (Tracing)

Contact tracing follows the logic of services traditionally used by health services: "it is any written record that identifies a patient and follows his or her medical history, which is monitored by health workers, who in turn can deliver medical recommendations personally or technically" (Weidenslaufer, C. and Meza, M. 2020, p. 1).

New ways to design applications have emerged in the environment, with the purpose that they collaborate beyond a simple localization. We refer to those applications that manage to do a work of tracing and not only tracking, previously developed. The objective to which they are oriented is not only to track patients, but also to alert those who have been physically close to a patient of COVID-19 to adopt the most appropriate sanitary measures necessary to help contain the spread of the virus (Weidenslaufer, C. and Meza, M. 2020, p. 1).

It is practically impossible for a subject to remember, and to know, all the contacts he or she may have had over a period of two days to a week after showing symptoms. The important thing is to break the chain of transmission of infection as effectively as possible. And this can be done by contact tracing apps (Arenas, M. 2020, p.3).

[15] Classification proposed by the Spanish Data Protection Agency.

In tracing type apps whose predominant technology is Bluetooth, what is of interest is not so much the exact location of the person, but to register the possible people with whom they have been in contact so that when someone tests positive, everyone else is alerted and thus detect asymptomatic people (Cascón-Katchadurian, 2020, p. 10). One of the advantages of these bluetooth applications is that they are anonymous and decentralized in general, so users would be told that they have been in contact with a patient who has tested positive but will not reveal the identity of the person (Cascón-Katchadurian, 2020, p. 15).

It should be noted that the fact that States monitor their population by their geolocation helps to provide assistance at specific geographic points in a more prompt and effective manner; however, it should not be considered that this is free of affectations to the fundamental right to the protection of personal data due to the practices that may result from the objective described above. The latter has been identified by Access Now[16], noting that "tracking the geographic location of smartphones provides information about the movement of people's phones rather than the virus" (2020, p. 10), and that tracking how COVID - 19 evolves by cross-referencing people's geographic data with cases of infection carries inherent risks (2020, p. 10).

The aforementioned organization also refers that, although the information that is recorded through tracking and tracing apps is anonymous, such characteristics can be reversed so that people can be easily re-identified, and that the information may be incomplete with respect to the place where the person carries out his or her activities (Access Now, 2020, p. 10),

The risks and the possible affectation to the right to the protection of personal data of this type of solutions can be produced when maps of relationships between people are made, re-identification by implicit location of the fragility of the protocols when configuring almost anonymous cards, and when the signals of the contagions are dispersed in such a way that the identity of the infected is not identified in any case.

3. Mass Temperature Measurement in Public Spaces

As fever is the most recurrent symptom in those infected by COVID-19, temperature scanning in people is especially relevant (Wilches-Visbal et al, 2021). Thus, one of the ways of mass temperature measurement in public spaces has been through thermal cameras with facial recognition.

Thermal cameras are devices that "detect the infrared radiation emitted by anybody with a temperature above absolute zero and transform it into an electrical signal, which is then processed to obtain a value or a temperature map" (Wilches - Visbal et al, 2020, pp. 305-306). As the AEPD points out, "(...) they add the ability to take the

[16] Access Now is non-profit organization that has been operating since 2009. Its mission is to defend the digital rights oft he world´s users.

temperature of individuals crossing an area, in many cases without requiring any action on their part" (2020a, p. 11).

In this regard, although the use of thermal cameras involves the use of an interesting technology to identify contagion, it can become a practice that compromises the personal data of individuals if it goes hand in hand with facial recognition, as Van Natta et al. have argued: "In such exceptional times, one could argue that fever checks offer substantial population health benefits with limited long-term impacts on personal privacy. Yet, several private companies have integrated thermal imag-ing with facial recognition technology". [In such exceptional times, one could argue that fever checks offer substantial population health benefits with limited long-term impacts on personal privacy. However, several private companies have integrated thermal imaging with facial recognition technology] (2020, p. 5).

In the field of work and, in particular, in occupational health and safety regulations, temperature taking can be useful, but placed in a more extensive data processing framework of which other additional checks and guarantees are part, in which the rights and freedoms provided for in the personal data protection regulations are respected (AEPD, 2020a, p. 12).

In Peru, Article 49 (c) of Law No. 29783, the Occupational Safety and Health Act, states that it is the employer's obligation to "identify any changes that may occur in working conditions and to make the necessary arrangements for the adoption of measures to prevent occupational hazards". This obligation means that the employer must pay particular attention to the measures he takes to ensure that his workers are in a situation of controlled risk in their workplace.

Regarding the risks to the possible impact on the right to the protection of personal data, it should be noted that the thermal camera and data collection can only be understood as part of a larger treatment and cannot take a person's health data and treat it spontaneously by any manager of a public place simply because he believes it is the best for his customers and users (AEPD, 2020a, p. 12), which can directly affect the principle of purpose.

It is also particularly problematic not to have the possibility of knowing the scope of the information that can be obtained using personal health data collected through this technological tool, because it may be information based on temperature measurement that reveals sensitive information about the health status of the person, such as pregnancy, menopause or the use of drugs, which would directly affect the principle of proportionality in the protection of personal data (Van Natta et al., 2020, p. 7).

In the absence of adequate regulation, such inaccurate monitoring can inadvertently cause harm to individuals who are labelled in a shopping mall during a trip without the slightest possibility of rectification (Van Natta et al., 2020, p. 8), which is a violation of the principle of quality. There will also be a risk of discrimination, stigmatization, and perhaps public dissemination of health data. All this can be aggravated by the risk

of leaks of sensitive information if the principle of security in the protection of personal data is not considered.

IV. By way of Conclusion

What has been developed in this paper leads to a reflection on the care that States and the private sector should take when adopting measures to address the expansion of COVID-19, which may have irreversible consequences on the fundamental right to the protection of personal data and which may be guided only by urgency, fear and, what is worse, by other interests.

As a result of the pandemic, States and individuals have implemented various technological tools to protect public health and prevent the spread of contagion. However, in certain cases, the implementation of these tools leads to assume risks and affectations to the right to the protection of personal data.

Having verified the existence of these risks, it is pertinent to rescue what is considered by the previously discussed resolution of the IACHR, insofar as it recommends to the governments of the Member States that they should guide their actions in accordance with two general obligations related to the protection of personal data:

> 35. Protect the right to privacy and personal data of the population, especially sensitive personal information of patients and individuals undergoing testing during the pandemic. States, health care providers, businesses, and other economic actors involved in pandemic containment and treatment efforts should obtain consent when collecting and sharing sensitive data from such individuals. They should only store personal data collected during the emergency for the limited purpose of combating the pandemic, without sharing it for commercial or other purposes. Affected individuals and patients will retain the right to erasure of their sensitive data.
>
> 36. Ensure that, where digital surveillance tools are used to identify, monitor or contain the spread of the epidemic and track affected individuals, they must be strictly limited, both in terms of purpose and time, and rigorously protect individual rights, the principle of non-discrimination and fundamental freedoms. States must make transparent the surveillance tools they are using and their purpose, as well as put in place independent oversight mechanisms for the use of these surveillance technologies, and secure channels and mechanisms for receiving complaints and grievances.

As can be seen, there are various risks associated with applications that provide information about the virus or facilitate self-diagnosis by the user. However, it is the responsibility of States and companies to provide proper management of the personal data of the users of the applications to achieve the objectives of providing information and care in the pandemic efficiently and respectful of the principles of the fundamental right to the protection of personal data.

It is for this reason that the guarantee of the fundamental right to the protection of personal data must be reinforced through an adequate design of technological tools and new models of information management, which means that not only experts in information systems, but also data scientists, specialists in artificial intelligence, bioethics, biolaw and human rights must participate in their development.

The processing of personal data in the current health emergency must have an overall objective based on scientific evidence, in which its proportionality has been assessed in relation to its effectiveness, efficiency and considering, in an objective manner, the necessary organizational resources.

V. Bibliography

Arias, M. (2016). Definitions for the purposes of the General Data Protection Regulation. In J.L. Piñar (Dir.) Reglamento general de protección de datos. Towards a new European privacy model (115-134). Reus.

Access Now. (2020). Recommendations for privacy and data protection in the fight against COVID-19. 28. Available at: https://www.accessnow.org/cms/assets/uploads/2020/04/Recommendations-for-the-protection-of-privacy-and-data-in-the-fight-against-COVID-19.pdf

Spanish Data Protection Agency (AEPD). (2020). Report N/Ref. 0017-2020 on the processing of personal data in relation to the spread of the COVID-19 virus.

Spanish Data Protection Agency (AEPD). (2020a). Report on the use of technologies in the fight against COVID-19. A cost-benefit analysis.

Spanish Data Protection Agency (AEPD). (2018). Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD [Guide].

Almada, M., & Maranhão, J. (2021). Voice-based diagnosis of covid-19: Ethical and legal challenges. International Data Privacy Law, 11(1), 63-75. Accessed April 15, 2021. Available at:https://doi.org/10.1093/idpl/ipab004

Alva, V. (2020). The COVID-19 pandemic, social distancing, the use of information and communication technologies and the lack of international regulation that protects personal data. Academic Journal of the Faculty of Law of La Salle University. Date of consultation: June 28, 2021. Available at: https://repositorio.lasalle.mx/handle/lasalle/1695

Andreu Martínez, B. (2020). Privacy, geolocation and contact tracing applications in the public health strategy generated by COVID-19. Actualidad Jurídica Iberoamericana 12, pp. 848-859.

Angarita, N. R. (2012). Constitutional approach to personal data protection in Latin America. International Journal of Personal Data Protection, 13.

Angarita, N. R. (2010). (2010). Does Colombia have an adequate level of personal data protection in light of the European standard? International Law: Colombian Journal of International Law, 8(16).

Arenas, M. (2020): Testing, Tracing, Isolation? On the Guidelines 04/2020 of the European Data Protection Committee. LA LEY Privacy, 4.

Arenas, M. (2020): To track or not to track? That's the question. Contact tracking apps and the protection of personal data. LA LEY Privacy, 5.

National Authority for the Protection of Personal Data. (2019). Advisory Opinion No. 07-2019-JUS/DGTAIPD-DPDP. Limitations to consent when processing health-related data, pursuant to Article 14, paragraph 6, of Law No. 29733. 06 February.

Biometric Vox (2020). Biometric Vox initiates research with artificial intelligence to de tect COVID19 through voice. Available at: https://biometricvox.com/blog/general/biometriricvox-initiates-investigation-artificial-intelligence-detect-covid19-by-voice/

Bizberge, A. and Segura, M.S. (2020). Digital rights during the COVID-19 pandemic in Argentina, Brazil and Mexico. Journal of Communication. 19 (2) pp. 61- 85.

Buchland Gidumal, J. (2020). Are geolocation apps reliable? The Conversation. Accessed May 23, 2021. Available at: https://theconversation.com/son-fiables-las-aplicaciones-de-geolocalizacion-y-seguimiento-de-contactos-141069

Cascón-Katchadourian, Jesús-Daniel (2020). Technologies to fight the Covid-19 pandemic: geolocation, tracking, big data, GIS, artificial intelligence and privacy. Information Professional, v. 29, n. 4, e290429. https://doi.org/10.3145/epi.2020.jul.29.

Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century.

Corredor, F. A., Suárez, J. C., & Patarroyo, L. J. (2020). Protección De Datos Personales en Sistemas De Monitorización y Vigilancia Masiva De Personas Ante La Pandemia De Covid-19.

Inter-American Court of Human Rights. (2020). Resolution 1/20: Pandemic and Human Rights in the Americas.

Cristea, L. (2018). The protection of sensitive data: digital health records and Big Data in Health. Bosch

Cubillos Sánchez, M. C., and Restrepo Rojas, M. A. (2020, December 7). CoronAPP-Colombia and its data processing policy. Computer Law Department. https://derinformatico.uexternado.edu.co/coroappcolombia/

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International Journal of Information Management, 55, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Domínguez, J. (2020). The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the longed-for technological development in the face of COVID-19. Journal of Communication and Health, 10(2), pp. 607-624.

European Data Protection Board (EDPB). (2020). Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted 19 March 2020. Accessed 17 May 2021 Available at:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_es_1.pdf

Herrera Bravo, R. (2011). Cloud computing and security: Clearing clouds to protect personal data. Journal of Law and Criminal Science: Social and Political Science, (17), 43-58.

Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., Rosero de los Ríos, D., Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., & Rosero de los Ríos, D. (2020). The right to the protection of personal data, digital technologies and COVID-19 pandemic in Colombia. Journal of Bioethics and Law, 50, 271-294.

Lopez, Luis Felipe (2016). Personal data protection: necessary adaptations to the new European Regulation. Francis Lefebvre.

Martinez, Ricard. (2020). To death by data protection. Accessed on: 20 April 2021. Available at: http://lopdyseguridad.es/a-la-muerte-por-proteccion-de-datos/

Mendoza Enriquez, O. A. (2018). Legal framework for the protection of personal data in service companies established in Mexico: challenges and compliance. IUS Journal, 12(41), 267-291.

United Nations. Human Rights Council. (2020). Press release. COVID-19: States must not abuse emergency measures to repress HRDs. 16 March. Accessed 17 May 2021. Available at:

Oliver, N., Lepri, B., Sterly, H., Lambiotte, R., Deletaille, S., De Nadai, M., ... & Vinck, P. (2020). Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. Sci Adv 6 (23) Accessed May 24, 2021. Available in:

https://advances.sciencemag.org/content/advances/6/23/eabc0764.full.pdf

Piñar, José Luis. (2020). Data protection during the coronavirus crisis. General Council of Spanish Lawyers. Accessed on: 20 April 2021. Available at: https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/

Puyol, J. (2016) XI. The principles of the Right to Data Protection. In José Luis Piñar (Dir.), Reglamento General de Protección de Datos. Madrid, pp. 135-150

Razquín, M. (2019). The necessary balance between transparency and protection of personal data. In Diego Zegarra Valdivia (Coord.), La proyección del derecho administrativo peruano: estudios por el centenario de la Facultad de Derecho de la PUCP. Lima, Palestra, pp. 137-164.

Recuero Linares, M. (2020). The international sharing of personal health-related data in times of COVID-19: Ethical and legal aspects for boosting the necessary cooperation. Journal of Bioethics and Law, 50, 133-146.

Renda, A. (2020). Will privacy be one of the victims of COVID-19? Centre for European Policy Studies. Published 23 March 2020. Available at:

Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J.R., Raisaro, J.L., Hubaux, J.P:, Fellay, J., & Vayena E. (2020). Data protection and ethics requirements for multisite research with health data: a comoaratove examination of legislative governance frame-works and the role of data protection technologies. Journal of Law and the Biosciences, 1-30. https://doi.org/10.1093/jlb/lsaa010

Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. Journal of Law and the Biosciences, 7. https://doi.org/10.1093/jlb/lsaa038. https://doi.org/10.1093/jlb/lsaa038

Vásquez Rodríguez, R. (2020). El consentimiento para tratamiento de datos personales de salud en tiempos del covid-19. Yachaq Revista De Derecho, (11), 145-164. https://Doi.Org/10.51343/Yq.Vi11.366

Visbal, J. H. W., Pedraza, M. C. C., & Veliz, D. G. A. (2021). Procedure for the usage of pyrometers during the COVID-19 pandemic: Procedure for the usage of pyrometers during the COVID-19 pandemic. Archivos de Medicina (Manizales), 21(1), 305-308.

Weidenslaufer, C. and Meza, M. (2020). COVID - 19: Use of apps with contact tracking and contact respect and privacy respect. Bulletin 10 Library of the National Congress of Chile /BCN. Available at: https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/79593/1/bulletin_coronavirus_10.1_FINAL.pdf

Wilches-Visbal, Jorge-Homero, & Castillo-Pedraza, Midian-Clara, & Apaza-Veliz, Danny-Giancarlo (2021). Procedure for the use of pyrometers during the COVID-19 pandemic. Archives of Medicine (Col), 21(1), 305-309.

Zegarra, D. (2014). The principles of personal data protection in the framework of Law No. 29733 and its Regulations. In Jorge Danós Ordóñez et al. (Coords.), Derecho Administrativo. Innovation, change and effectiveness. Libro de ponencias del Sexto Congreso Nacional de Derecho Administrativo. Lima, ECB Ediciones, pp. 623-635.

Zegarra, D. (2019). Peruvian personal data protection regulations facing the challenge of moving from a data management model to the responsible use of information. In Diego Zegarra Valdivia (Coord.), La proyección del derecho administrativo peruano: estudios por el centenario de la Facultad de Derecho de la PUCP. Lima, Palestra, pp. 165-208.