



Received 15/08/2020

Accepted 23/09/2020

THE NECESSARY PROTECTION OF SPECIAL CATEGORIES OF PERSONAL DATA. A REFLECTION ON HEALTH-RELATED DATA AS AN ESSENTIAL AXIOM TO ACHIEVE THE DESIRED TECHNOLOGICAL DEVELOPMENT IN THE FACE OF COVID-19

La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19

José Luis Domínguez Álvarez ¹

University of Salamanca. Spain.

jldoal@usal.es

Funding. *The present contribution is carried out under the auspices of the Program of Grants for the Training of University Teaching Staff (FPU17/01088) of the Ministry of Education, Culture and Sport. The author is a member of the Recognized Research Group "Reform and Modernization of Public Administrations" (GISALMAD-USAL).*

Abstract

The irruption of COVID-19 has led to a multitude of deep-seated transformations, which go beyond the purely sanitary sphere, leading to major socio-economic changes, among which the evolution of traditional forms of administrative intervention or the empowerment and/or acceleration of the advances derived from the digital (re)volution stand out for their extraordinary importance. Thereby, in recent months we have witnessed the implementation of numerous initiatives aimed to alleviate the harmful effects of the pandemic by developing technological tools based on processing categories of specially protected personal data, such as health data, which raises important questions from the perspective of privacy and digital rights. The aim of this study is to carry out a detailed analysis of some essential elements, necessary to achieve the difficult balance between the promotion of technological instruments that contribute to control the effects of COVID-19 increasing the resources available to health authorities, and safeguarding the fundamental right of personal data protection.

Keywords: COVID-19, protection data, privacy, technological development, health authorities, Radar COVID.

¹ **José Luis Domínguez Álvarez:** Research Staff in Training (FPU) of the Administrative Law Area of the University of Salamanca, specialized in the study of the protection of personal data in the digital (re)volution, the modernization of public administrations, sustainable rural development and the emptied Spain, as well as in the implementation of public policies of equality and fight against gender violence.

Resumen

La irrupción del COVID-19 ha propiciado el surgimiento de multitud de transformaciones de profundo calado, las cuales rebasan la esfera puramente sanitaria, propiciando importantes cambios socioeconómicos, entre los que destaca por su extraordinaria importancia la evolución de las formas tradicionales de intervención administrativa o el empoderamiento y/o aceleración de los avances derivados de la (re)volución digital. De esta forma, en los últimos meses hemos asistido a la implementación de numerosas iniciativas encaminadas a paliar los efectos nocivos de la pandemia sanitaria mediante el desarrollo de herramientas tecnológicas sustentadas en el tratamiento de categorías de datos personales especialmente protegidos, como son los datos relativos a la salud, lo que plantea importantes incógnitas desde la perspectiva de la privacidad y los derechos digitales. El presente estudio tiene por objeto realizar un análisis pormenorizado de las cuestiones esenciales necesarias para alcanzar el difícil equilibrio entre el impulso de instrumentos tecnológicos que contribuyan a controlar los efectos del COVID-19, incrementando los recursos a disposición de las autoridades sanitarias, y la salvaguarda del derecho fundamental a la protección de datos de carácter personal.

Palabras clave: COVID-19, protección de datos personales, privacidad, desarrollo tecnológico, autoridades sanitarias, Radar COVID.

How to cite the article

Domínguez Álvarez, J. L. (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. *Revista de Comunicación y Salud*, 10(2), 607-624. doi: [https://doi.org/10.35669/rcys.2020.10\(2\).607-624](https://doi.org/10.35669/rcys.2020.10(2).607-624).

1. INTRODUCTION

At the end of last year, a new outbreak of coronavirus (SARS-CoV-2) appeared in Hubei Province of the People's Republic of China, causing an enormous commotion among the medical community and the rest of the world (Velavan and Meyer, 2020). Despite the adoption of a multitude of health measures and different protocols, COVID-19 has ended up becoming an unprecedented pandemic in our recent history, leading to the saturation of health resources and causing enormous human, economic and social losses (Palacios Cruz, Santos, Velázquez Cervantes and León Juárez, 2020).

The European continent, and especially our country, have not been spared in any way from the devastating effects of the global pandemic², the harshness of which is

² On 11 March 2020, the World Health Organization upgraded the public health emergency caused by COVID-19 to an international pandemic.

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

reflected in a multitude of figures³ that hide behind them dramatic human, economic and social losses.

As is well known, in recent months digital technologies and data, especially in terms of mass processing of quantitative and qualitative data, have become of transcendental importance in the fight against the COVID-19 crisis (Martínez Martínez, 2020b). Certainly, these technologies and data offer in many cases an important tool to inform the public at large and assist the relevant public authorities in their efforts to contain the spread of the virus or to enable health organizations to exchange health data rapidly. However, as highlighted by the European Commission in its Recommendation 2020/518 on a common EU toolkit for the use of technology and data to combat and overcome the COVID-19 crisis, in particular with regard to mobile applications and the use of anonymised mobility data, a fragmented and uncoordinated approach to the use of new technologies based on the processing of personal data jeopardises the effectiveness of measures to combat the COVID-19 crisis, seriously damaging both the single market and fundamental rights and freedoms.

In this sense, many efforts have been made by the different public administrations to design mobile applications that can contribute to the monitoring and containment of the current health pandemic (Cotino Hueso, 2020)⁴. Encouraged by the multiple opportunities offered by these tools, including the possibility of providing guidance to citizens about social distancing measures, facilitating the organization of medical monitoring of patients or contact tracing, thereby limiting the spread of the disease and interrupting the chains of transmission; Indeed, combined with appropriate PCR testing strategies and contact tracing, the applications can be particularly important in providing information on the level of virus circulation, assessing the effectiveness of physical containment and containment measures, and guiding de-escalation strategies to expedite as much as possible the grim task of economic and social recovery that lies ahead.

Thus, it is not difficult to find different public and private initiatives⁵ aimed at the creation of web applications and resources closely related to the COVID-19 pandemic,

³ The case detection rate changes daily and can be tracked in near real time at the following website provided by Johns Hopkins University: <https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6>.

⁴ A good example of this can be found in Order SND/297/2020, of 27 March, which entrusts the Secretary of State for Digitalisation and Artificial Intelligence, of the Ministry of Economic Affairs and Digital Transformation, with the development of various actions for the management of the health crisis caused by COVID-19.

⁵ Following this trail of initiatives and movements in times of COVID-19, and taking into consideration the processing of personal data and, particularly, health-related data that many of these initiatives involve, the Spanish Data Protection Agency (AEPD) issued, on 26 March, a statement on the criteria that allow the use of these apps and web self-assessment of COVID-19 with the existing regulation on data protection. According to the indications provided by the AEPD, "only the public authorities competent to act in accordance with the declaration of the state of alarm, that is, the Ministry of Health and the Departments of Health of the Autonomous Communities, which may transfer data between them, and health professionals who treat patients or involved in the control of the epidemic may treat such data. The private

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

initiatives that in most cases are based on the processing of health data, or what is the same, on personal data specially protected under art. 9 RGPD. Within these technological applications we find two large groups, depending on their purpose and typology: alert and monitoring applications; and self-diagnosis and symptom analysis applications.

Regardless of the type of applications or tools to which we refer, what is certain is 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 win the battle against COVID-19, insofar as they allow improving the foresight and decision-making capacity of health authorities, contribute to strengthening the effectiveness of social distancing measures, thereby significantly reducing the spread of the pandemic, or by maximizing the desired administrative efficiency, an idea-force that our Constitution includes in its art. 103.1 as a guiding principle of the actions of public administrations, and that today more than ever is essential when strategically allocating health means and resources to minimize the human cost, which at this point is already insufferable (Terrón Santos, Domínguez Álvarez, and Fernando Pablo, 2020).

However, given the functions of the applications and tools enabled for smartphones, described above, their use is likely to affect the exercise of certain fundamental rights⁶ such as the right to respect for private and family life or the right to the protection of personal data, among others (Martínez Martínez, 2020a). The following pages analyse a series of essential issues necessary to achieve the difficult balance between the promotion of technological tools that contribute to controlling the effects of COVID-19, increasing the resources available to the health authorities, and safeguarding the fundamental right to the protection of personal data.

2. OBJECTIVES

The purpose of this study is to clear up, on the basis and premises of the old Rule of Law, the main unknowns surrounding the use of technology in times of anxiety, helping to clarify the difficult balance between technological development and guaranteeing the

entities that collaborate with these authorities may only use the data in accordance with their instructions and, under no circumstances, for purposes other than those authorised". AEPD official communiqué retrieved from: <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad>

⁶ A good example of this can be found in the mobile application, promoted by the Beijing government, known as "Health Code", a tool that was distributed on the popular platforms Alipay and WeChat to proceed with the collection of huge amounts of data relating to the mobility and health of citizens - far from the principles that should inform any processing of personal data on the European continent. This tool makes it possible to assign an identifying colour to each person, depending on the data entered by the individual. This code (green, yellow or red) determines the mobility of the individual, and can be required for verification by the authorities on public roads, at the entrances to commercial establishments or on public transport. According to experts, this application has played a crucial role in considerably reducing the spread of the pandemic in the Asian giant, while giving up the privacy of society as a whole, something extremely dangerous in the turbulent waters of the world of digitization and digitization.

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

fundamental rights of citizens, paying special attention to the protection of personal data. Without losing sight of the ultimate purpose of this legal guarantee, which has been conceived by the European Union with a strong humanistic inspiration, as the fourth recital of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) states lapidarily, "*the processing of personal data must be designed to serve humanity*".

3. THE REGULATION OF THE PROTECTION OF PERSONAL HEALTH DATA: POSSIBILITIES FOR ITS CORRECT TREATMENT

As has been pointed out by numerous theorists and academics, the declaration of the state of alarm decreed after the adoption of Royal Decree 463/2020, of 14 March, does not allow the limitation of rights and freedoms beyond the provisions of the aforementioned article 11 of Organic Law 4/1981 (Lozano Cutanda, 2020; Fernández de Gatta Sánchez, 2020), which in view has a series of implications from the point of view of the protection of personal data.

In general, both the European Data Protection Committee ⁷and the various supervisory authorities (Piñar Mañas, 2020b), including the AEPD, have issued statements regarding the processing of personal data in the context of the Covid-19 crisis. All these statements express a common sentiment, highlighting that data protection regulations and in particular Regulation (EU) 2016/679, do not prevent measures from being taken in the fight against the coronavirus pandemic, but warn that even in these exceptional circumstances those who process personal data must ensure their protection, especially if we take into account that in many cases such processing uses particularly sensitive data, such as data related to health, which are intimately and closely linked to the right to life (Troncoso Reigada, 2010).

⁷ Thus, the European Data Protection Committee in its statement on the processing of personal data in the context of the Covid-19 crisis, of 16 March, establishes the absence of impediments by the GDPR to proceed with the fight against the coronavirus pandemic, stating that: "*the GDPR is a broad legislation and also provides for the rules to apply to the processing of personal data in a context such as the one relating to COVID-19. Indeed, the GDPR provides for the legal grounds to enable the employers and the competent public health authorities to process personal data in the context of epidemics, without the need to obtain the consent of the data subject. This applies for instance when the processing of personal data is necessary for the employers for reasons of public interest in the area of public health or to protect vital interests (Art. 6 and 9 of the GDPR) or to comply with another legal obligation. For the processing of electronic communication data, such as mobile location data, additional rules apply. The national laws implementing the ePrivacy Directive provide for the principle that the location data can only be used by the operator when they are made anonymous, or with the consent of the individuals. The public authorities should first aim for the processing of location data in an anonymous way (i.e. processing data aggregated in a way that it cannot be reversed to personal data). This could enable to generate reports on the concentration of mobile devices at a certain location ("cartography"). When it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the member states to introduce legislative measures pursuing national security and public security. This emergency legislation is possible under the condition that it constitutes a necessary, appropriate and proportionate measure within a democratic society. If such measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals the right to judicial remedy*".

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

Under the current regulation, data relating to health represent what are known as special categories of personal data. It should be recalled that the GDPR qualifies as such those data that "by their nature are particularly sensitive in relation to fundamental rights and freedoms" (Recital 51). And the first paragraph of Article 9 of the GDPR essentially maintains the data that were already considered worthy of greater protection in Article 8 of Directive 95/46/EC: ethnic or racial origin; political opinions; religious or philosophical beliefs; trade union membership; health and sexuality, although with regard to the latter it now specifies: "data concerning sex life or sexual orientation" (Medina Guerrero, 2019).

For its part, art. 4.15) RGDPD specifies and clarifies the concept of "data relating to health", unlike Directive 95/46/EC, which did not address its conceptualization. According to this provision, data concerning health are understood as "personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her state of health".

Having clarified the above, it is important to clarify the legal regime and the possibilities of processing these health data, which as we have shown are essential to promote the sufficient technological development necessary to win the game against COVID-19.

In this regard, the first thing to note is that the GDPR itself, in recital 46, recognizes that, in exceptional situations, such as the one we are currently experiencing, the legal basis for processing may be multiple, based on both the public interest and the vital interest of the data subject or another natural person.

(46) 'The processing of personal data should also be considered lawful where it is necessary for the protection of an interest essential for the life of the data subject or that of another natural person. In principle, personal data should only be processed on the basis of the vital interest of another natural person where the processing cannot manifestly be based on a different legal basis. Certain types of processing may meet both important grounds of public interest and the vital interests of the data subject, such as where processing is necessary for humanitarian purposes, including the control of epidemics and their spread, or in humanitarian emergencies, in particular in the event of natural or man-made disasters'.

Therefore, as a legal basis for lawful processing of personal data (Puyol Montero, 2016), without prejudice to the existence of other bases, such as, for example, compliance with a legal obligation ex art. 6.1.c) GDPR, such as the processing of personal data carried out by the employer for the prevention of occupational risks of its employees; the GDPR explicitly recognizes two different legal bases for the lawful⁸ processing of personal data: the processing is necessary to protect the vital interests of

⁸ According to Recital 40 GDPR, "for processing to be lawful, personal data must be processed with the consent of the data subject or on some other legitimate basis laid down by law, whether in this Regulation or under other Union or Member State law referred to in this Regulation [...]."

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

the data subject or of another natural person -art. 6.1.d)-; and the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller -art. 6.1.e)-.

Art. 6.1, letter d) GDPR considers not only that the vital interest is sufficient legal basis of the processing to protect the data subject⁹, but that such legal basis can be used to protect the vital interests "of another natural person", which by extension means that such natural persons can be even unidentified or unidentifiable; that is to say, such a legal basis for processing - the vital interest - may be sufficient for processing of personal data aimed at protecting all those persons likely to be infected in the spread of an epidemic, which would justify, from the point of view of processing personal data, in the widest possible manner, the measures adopted for this purpose, even if they are aimed at protecting unnamed or in principle unidentified or unidentifiable persons, insofar as the vital interests of these natural persons must be safeguarded, and this is recognised by the personal data protection regulations (Spanish Data Protection Agency, 2020).

Based on the above, it does not seem strange that this legal basis for processing has traditionally been linked to that established in Article 9.2 c) of the GDPR, insofar as it allows lifting the prohibition of processing of the special categories of data regulated by it when the processing is necessary to protect the vital interests of the data subject or of another natural person, in the event that the data subject is not physically or legally able to give consent (Puente Escobar, 2019).

However, for the processing of health-related data, it is not enough that there is a legal basis in Art. 6 RGD, but according to Art. 9.1 and 9.2 RGD there must necessarily be a circumstance that lifts the prohibition of processing of this special category of data (Martínez Martínez, 2020^a).

In the specific case in which we find ourselves, these circumstances should be sought in several of the sections outlined in art. 9.2 RGD. Thus, the prohibition to proceed with the processing of personal data related to health will not operate in the following cases:

First, pursuant to point (b) of that provision, where processing is necessary for the purposes of the performance of obligations and the exercise of specific rights of the controller or of the data subject in the field of employment law, social security and social protection, in so far as authorised by Union law of the Member States or by a collective agreement under the law of the Member States providing for appropriate safeguards for the respect of the fundamental rights and interests of the data subject.

Second, pursuant to Art. 9.2.g) GDPR, where processing is necessary for reasons of essential public interest, on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect in essence the right to data protection and

⁹ Pursuant to art. 4.1) RGD, a data subject is any identified or identifiable natural person.

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

provide for adequate and specific measures to protect the interests and fundamental rights of the data subject.

Third, pursuant to point (i), where the processing of this set of particularly sensitive data 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.

Fourthly, and in line with the provisions of letter h), when the treatment is necessary for a medical diagnosis, or assessment of the worker's capacity to work or any other type of health care or for the management of health and social care systems and services.

To these exceptions, the AEPD considers it necessary to add a fifth and final closing circumstance which would allow the processing of health-related data. In this way, according to the Agency's criteria, "it could even be the one established in letter c), in the event of the circumstances set out in this section, which would apply when the processing is necessary to protect the vital interests of the data subject or of another natural person, in the event that the data subject is not physically or legally able to give consent" (Agencia Española de Protección de Datos, 2020).

Consequently, in a health emergency situation such as the one we are in, it should be borne in mind that, within the exclusive scope of personal data protection law, the application of personal data protection law would allow the controller to take those decisions that are necessary to safeguard the vital interests of natural persons, the fulfilment of legal obligations or the safeguarding of essential interests in the field of public health, provided that the essential content of the right to data protection is respected and adequate¹⁰ and specific measures are established to protect the interests and fundamental rights of the data subject (Piñar Mañas, 2020^a).

In this regard, data controllers, in order to guarantee their correct performance and effectively safeguard the vital interests of citizens, must act in accordance with the instructions provided by the health authorities, by virtue of what is established in the sectoral regulatory provisions for this purpose.

¹⁰ In accordance with the principle of proactive responsibility -art. 5.2 GDPR-, and the principles of data protection by design and by default -art. 25 GDPR-, appropriate technical and organisational measures, such as pseudonymisation, and even aggregation and anonymisation of health-related data, must be adopted both at the time of determining the means of processing and at the time of the processing itself. Furthermore, in accordance with the principle of data minimisation - Art. 5.1.c) GDPR - it must be ensured that, by default, only personal data which are necessary for each of the specific purposes of the processing and which will not be accessible, without the intervention of the individual, to an indeterminate number of persons are processed.

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

It should be pointed out that our legal system, which is criticised by some, establishes a series of legal provisions that are necessary and appropriate to deal with situations of health risk such as the scenario caused by the outbreak of COVID-19. We are referring, as it could not be otherwise, to the Organic Law 3/1986, of 14 April, on Special Measures in Public Health (amended by Royal Decree-Law 6/2020, of 10 March, adopting certain urgent measures in the economic field and for the protection of public health, published in the Official State Gazette of 11 March 2020) and Law 33/2011, of 4 October, General Law on Public Health.

In this regard, art. 3 of LO 3/1986 establishes that:

["In order to control communicable diseases, the health authority, in addition to general preventive actions, may adopt appropriate measures for the control of the sick, of persons who are or have been in contact with them and of the immediate environment, as well as those considered necessary in cases of risk of a communicable nature".

For its part, art. 54.1 of Law 33/2011, of 4 October, General Law on Public Health (LGSP), establishes the following:

["Without prejudice to the measures provided for in Organic Law 3/1986, of 14 April, on Special Public Health Measures, exceptionally and when required for reasons of extraordinary gravity or urgency, the General State Administration and those of the Autonomous Communities and the cities of Ceuta and Melilla, within the scope of their respective competences, may adopt any measures¹¹ necessary to ensure compliance with the law".

Therefore, with regard to communicable diseases, the above-mentioned sectoral health regulations grant the health authorities the necessary powers to adopt the necessary measures provided for in those laws when so required for urgent or necessary health reasons.

Consequently, from the point of view of the processing of personal data, the safeguarding of essential public health interests is the responsibility of the various health authorities of the different public administrations, which may adopt the necessary measures to safeguard these essential public interests in situations of public health emergency.

¹¹ Thus, according to the legislator's criteria, by virtue of art. 54.2 LGSP, "the competent authority may adopt, by means of a reasoned resolution, the following measures: a) The immobilisation and, if appropriate, the confiscation of products and substances; b) The intervention of material or personal means; c) The preventive closure of the installations, establishments, services and industries. d) The suspension of the exercise of activities; e) The determination of prior conditions at any stage of the manufacture or marketing of products and substances, as well as the operation of facilities, establishments, services and industries referred to in this law, in order to correct the deficiencies detected; f) Any other measure in accordance with current legislation if there are reasonable indications of risk to health including the suspension of actions in accordance with the provisions of Title II of this law".

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

In this way, these same health authorities will be responsible for ensuring the correct processing of personal data, in accordance with the requirements and obligations established in the regulations on the protection of personal data. Especially with regard to strict compliance with the principles set out in art. 5 RGPD, including the principle of lawful, fair and transparent processing of personal data, purpose limitation ¹²(in this case, to safeguard the vital/essential interests of natural persons), the principle of accuracy, and of course, and this should be particularly emphasized, the principle of data minimization, the importance of which has already been mentioned above, ensuring that the data processed will be exclusively those necessary for the intended purpose, without extending such processing to any other personal data not strictly necessary for that purpose, without confusing convenience with necessity, because the fundamental right to data protection continues to apply normally, without prejudice to the fact that, as has been said, the personal data protection regulations themselves establish that in emergency situations, for the protection of essential public health and/or vital interests of natural persons, the health data necessary to prevent the spread of the disease that has caused the health emergency may be processed (Spanish Data Protection Agency, 2020).

4. "RADAR COVID", SPAIN'S BID TO HALT THE SPREAD OF THE PANDEMIC AND SAFEGUARD CITIZENS' PRIVACY RIGHTS

As we have noted above, many efforts have been made by the different public administrations in recent months to seek innovative solutions that would contribute, on the one hand, to increase the resources made available to the public health system, and on the other, to try to control the enormous and rapid expansion of the pandemic, which far from diminishing as the de-escalation measures progress, threaten to provoke a second wave of contagion, even more bloody than the previous one if possible. It is in this context in which the work of promoting and implementing the Radar COVID app is framed, which, despite its late launch, is fully operational in many Autonomous Communities of the Spanish geography, among which are Andalusia, Cantabria, Aragon, Canary Islands, Extremadura, Balearic Islands and Castilla y León.

The following lines analyse the main advantages and potentialities of this new tool, with the aim of improving and deepening citizens' knowledge of it, an essential element to guarantee its full effectiveness.

¹² Recital 54 GDPR is clear in this respect: "the processing of special categories of personal data, without the consent of the data subject, may be necessary for reasons of public interest in the area of public health. Such processing must be subject to appropriate and specific measures in order to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, determinants influencing health status, health care needs, resources allocated to health care, provision of and universal access to health care, health care expenditure and financing, and causes of mortality. Such processing of health-related data for reasons of public interest should not result in third parties, such as employers, insurance companies or banking institutions, processing personal data for other purposes.

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

4.1. What is COVID Radar?

Radar COVID is an application for mobile devices for SARS-CoV-2 virus contagion alert developed by the Government of Spain, whose owner is the General Secretariat of Digital Administration, under the Secretary of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation.

Thanks to this novel tool, those users who have downloaded the application and accept its use will receive a notification in the event that in the fourteen days prior to that notification they have been exposed to an epidemiological contact -within two meters and more than 15 minutes- with another user -totally anonymous- who has declared in the application to have given a positive result in the COVID-19 test, prior accreditation by the corresponding health authorities. This tool will inform users exclusively about the day, within the previous fourteen days, on which exposure to the virus has occurred, safeguarding the identity of the user who has been exposed and protecting the identification of the user's device. In this way, it has been possible to articulate a digital tool that exponentially maximizes the ability to track the spread of the virus of the health authorities while establishing high standards of privacy protection, since the application does not request, use or store personal data of users, as is clear from both its privacy policy and the statements of those responsible for this digital tool.

At this point, it should be stressed that the success of the application as a decisive tool aimed at making a significant contribution to the efforts to contain the spread of the virus is directly linked to the degree to which it is used by the population. Hence the need to promote public awareness in order to maximize the scope and impact of a technological tool that respects fundamental rights and that stands as a crucial weapon to mitigate the pernicious effects of the second wave of the pandemic that is about to arrive, a task not without difficulty in which both the media and communication professionals can and should play a fundamental role.

4.2. How does Radar COVID work?

One of the main potentialities of the Spanish COVID-19 app is its simple and intuitive design. Once the user has proceeded to download the application, either from the App Store or Google Play depending on the operating system of the device, has accepted the terms of use and privacy policy and starts using it, the mobile device will generate every day a pseudo-random identifier known as "temporary exposure key" with a size of 16 characters (16 bytes or 128 bits) that will serve to derive the "Bluetooth ephemeral identifiers" that are exchanged with other nearby mobile phones that also have downloaded the Radar COVID application.

Now, what are the so-called "Bluetooth ephemeral identifiers" on which the aforementioned app is based? These identifiers are a series of pseudo-random codes with a size of 16 characters (16 bytes, or 128 bits), which are generated by each of the different mobile devices every 10-20 minutes, from the daily "temporary exposure key".

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

The most relevant thing about these codes is that they do not contain any personal information that would directly or indirectly identify the device or its user, thereby protecting the data relating to the health of patients at all times, which makes this digital tool an effective mechanism to expand the tracking capacity of the health authorities in terms of the spread of the virus, while standing as a respectful instrument for the fundamental rights of citizens, and especially as regards our object of study, the protection of personal data.

Additionally, it is necessary to know that these "Bluetooth ephemeral identifiers" are transmitted by smartphones several times per second to nearby devices, accessible through Bluetooth Low Energy technology, producing an exchange of random codes between devices so that they can be stored by nearby phones that have downloaded the application. All this with the aim of calculating whether the user has been in contact with someone who has been infected by COVID-19 over the last 14 days.

Similarly, Radar COVID provides the possibility of communicating through the aforementioned tool the receipt of a positive diagnosis by COVID-19, by voluntarily entering in the application the "single-use confirmation code" that will be previously provided by the Public Health Service and that will be validated in the app server. Subsequently, the application will request the user's express consent to send to the server the last 14 temporary exposure keys stored on the device in question, which will be used to compile a daily list of temporary exposure keys of people infected by COVID-19 that will be downloaded daily from the server by all COVID Radar applications that are in operation to ensure the full effectiveness of the technological product. That is, the application periodically downloads the temporary exposure keys voluntarily shared by COVID-19 diagnosed users from the server, to compare them with the random codes registered in the previous days as a result of contacts with other users. If a match is found, the application runs an algorithm on the device that, depending on the duration and estimated distance of the contact, and according to the criteria established by the health authorities, decides whether to display a notification on the device of the user exposed to the risk of contagion, warning him of the contact, informing him of the date of the contact and inviting him to self-confirm, and contact the health authorities.

It is in this phase where the media and communication professionals are of paramount importance when it comes to informing the population about the advantages and potential of making responsible and complete use of the Radar COVID application. While it is true that the health authorities continually insist on the need to maximize the download and installation of the application on as many mobile terminals as possible, this action represents just one of the actions that we as citizens can develop to properly use the tool and thus contribute to facilitate the work of tracking and control of the spread of the pandemic. In this sense, it is equally or even more important to use the function of communicating a positive diagnosis after undergoing the mandatory test prescribed by the health authorities, since this is the only way to maximize the effectiveness of the digital application, and with it the deployment of the multiple advantages derived from its implementation.

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

In short, the Radar COVID app is an additional tool aimed at expanding the resources available to the public health system to address a health challenge of unknown proportions, whose success depends largely on the response that citizens give when making a responsible and complete use of the functions articulated by the health authorities, an issue that depends on the dissemination and information that public administrations and the media make available to the population.

5. CONCLUSIONS

The vertiginous technological development is nowadays presented as a powerful tool, capable of contributing significantly to the complex decision-making processes of the health authorities aimed at overcoming the "alarm" situation caused by COVID-19, a pandemic that has caused devastating effects, leaving behind a painful trail of human and socio-economic losses, and that has hit the pillars of the European Union, even calling into question the very values inherent to the concept of European citizenship.

But beyond these visible devastating effects, COVID-19 has raised important unknowns or questions that have led to the creation of important debates in which, on many occasions, the very validity and effectiveness of the social and democratic rule of law has come to be at stake. An example of these fierce debates can be found in the virulent confrontation that some academic, political and social sectors have raised between public health and personal data protection in reductionist terms, wielding a series of tautological arguments that advocated the fervent defence of public health to the detriment of the fundamental rights of privacy, which, as we have pointed out, not only cannot be suspended in any way through the declaration of a State of Alarm, but constitute the very foundation of the set of constitutionally recognized rights in the face of the growing processes of digitization and datification of society.

In our opinion, it is not true that the protection of personal data and its powerful regulation presided over by the GDPR are presented as obstructionist elements, leading to hinder the implementation and performance of personal data processing necessary for the adoption of effective measures against COVID-19; Nothing could be further from the truth, what is being pursued, as we have made clear in the preceding pages, is the correct application of an advanced regulation of a fundamental right, data protection, which, let us remember, includes among its provisions the performance of personal data processing actions in atypical or supervening scenarios such as the one in which we find ourselves. Therefore, from our point of view, perhaps impregnated by the historical development and the marked humanist character of the Salamanca study, the confrontation between public health and data protection is not such, but rather the opposite: both issues are indissoluble elements of the same equation. In a context of emergency such as the one we are living in, it is impossible to achieve a certain guarantee of public health without safeguarding high standards of personal data protection, the latter right which, as we have already insisted, constitutes the basic

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

institute for the full effectiveness and guarantee of the set of constitutionally recognised fundamental rights, standing as the cornerstone of the social and democratic State of Law in the face of the digital revolution.

A good example of this necessary connivance between technological development and safeguarding the fundamental right to the protection of personal data can be found in the implementation of the Spanish application Radar COVID, which, despite its late launch, aspires to be an essential tool in the hands of the health authorities to control once and for all the spread and extension of the health pandemic. However, it should be noted that the effectiveness and usefulness of this application is closely and directly linked to the full and responsible use by the public, an issue in which the media and communication professionals acquire a transcendental importance, becoming indispensable agents to provide accurate and truthful information to the population as a whole.

6. REFERENCES

Spanish Data Protection Agency (2020). *Legal Report 0017/2020*, Madrid. Retrieved from <https://www.aepd.es/es/documento/2020-0017.pdf>

Cotino Hueso, L. (2020). Intelligència artificial, big data i aplicacions contra la Covid-19, i la privacitat i protecció de dades. *IDP Revista de Internet, Derecho y Política*, (31). doi: [10.7238/idp.v0i31.3244](https://doi.org/10.7238/idp.v0i31.3244).

European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEU § L-1995-81678 (1995). [DOUE § L-1995-81678](#)

Fernández de Gatta Sánchez, D. (2020). Los problemas de las medidas jurídicas contra el coronavirus: las dudas constitucionales sobre el Estado de Alarma y los excesos normativos. *Diario La Ley*, (9634). Retrieved from <https://diariolaley.laleynext.es/dli/2020/05/18/los-problemas-de-las-medidas-juridicas-contra-el-coronavirus-las-dudas-constitucionales-sobre-el-estado-de-alarma-y-los-excesos-normativos>

Lozano Cutanda, B. (2020). Análisis de urgencia de las medidas administrativas del estado de alarma. *Diario La Ley*, (9601). Retrieved from <https://diariolaley.laleynext.es/dli/2020/03/25/analisis-de-urgencia-de-las-medidas-administrativas-del-estado-de-alarma>

Martínez Martínez, R. (2020a). Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. *Diario La Ley*, 38(1). Retrieved from <https://diariolaley.laleynext.es/dli/2020/03/27/los-tratamientos-de-datos-personales-en-la-crisis-del-covid-19-un-enfoque-desde-la-salud-publica>

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

Martínez Martínez, R. (2020b Covid-19 ¿hacia un rediseño de la privacidad? *La Ley Privacidad*, (5). Retrieved from <https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAEAMtMSbF1jTAAAkNTUzMMDM7Wy1KLizPw827DM9NS8kIS15JzUxCKXxJJU58Sc1LyUxCLbkKLSVACvPbJxNwAAAA==WKE>

Medina Guerrero, M. (2019). Special categories of data. In A., Rallo Lombarte (Ed.) *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 251-274). Valencia, Spain: Tirant lo Blanch.

General Public Health Law 33/2011, BOE § A-2011-15623 (2011). ELI: <https://www.boe.es/eli/es/l/2011/10/04/33/con>

Organic Law 4/1981 on states of alarm, exception and siege, BOE § A-1981-12774 (1981). ELI: <https://www.boe.es/eli/es/lo/1981/06/01/4/con>

Organic Law 3/1986 on Special Public Health Measures, BOE § A-1986-10498 (1986). ELI: <https://www.boe.es/eli/es/lo/1986/04/14/3/con>

Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights, BOE § A-2018-16673 (2018). ELI: <https://www.boe.es/eli/es/lo/2018/12/05/3>

Order SND/297/2020 entrusting the Secretary of State for Digitalization and Artificial Intelligence, of the Ministry of Economic Affairs and Digital Transformation, with the development of various actions for the management of the health crisis caused by COVID-19, BOE § A-2020-4162 (2020). ELI: <https://www.boe.es/eli/es/o/2020/03/27/snd297>

Palacios Cruz, M., Santos, E., Velázquez Cervantes, M. A., & León Juárez, M. (2020). COVID-19, una emergencia de salud pública mundial. *Revista Clínica Española*, S0014-2565(20), 30092-8. doi: <http://doi.org/10.1016/j.rce.2020.03.001>.

Piñar Mañas, J.L. (2020a). Privacidad en estado de alarma y normal aplicación de la Ley. *Hay Derecho*. Retrieved from: <https://hayderecho.expansion.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/>

Piñar Mañas, J.L., (2020b). Los peligros de una república digital desbocada. A propósito del Real Decreto-Ley 14/2019, de 31 de octubre, en materia de administración digital, contratación del sector público y telecomunicaciones. *Revista Derecho Digital e Innovación*, (3).

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

Piñar Mañas, J.L., (2020c).). Transparencia y protección de datos en el estado de alarma y en la sociedad digital post COVID-19. En D. Blanquer, *Covid-19 y Derecho Público (durante el estado de alarma y más allá)* Valencia, Spain: Tirant lo Blanch.

Puente Escobar, A. (2019). Principios y licitud del tratamiento. En A., Rallo Lombarte (Ed.) *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 115-168). Valencia (pp. 115-168). Valencia, Spain: Tirant lo Blanch.

Puyol Montero, J. (2016). Los principios del derecho a la protección de datos. En J.L., Piñar Mañas, M.A., Caro, M., Recio Gayo (Ed.) *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (pp. 135-150). Madrid, Spain: Editorial Reus.

Royal Decree 463/2020 declaring a state of alarm for the management of the health crisis situation caused by COVID-19, BOE § A-2020-3692 (2020). ELI: <https://www.boe.es/eli/es/rd/2020/03/14/463/con>

Royal Decree-Law 6/2020 adopting certain urgent measures in the economic field and for the protection of public health, BOE § A-2020-3434 (2020). ELI: <https://www.boe.es/eli/es/rdl/2020/03/10/6/con>

European Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolkit for the use of technology and data to combat and overcome the COVID-19 crisis, in particular as regards mobile applications and the use of anonymised mobility data, OJEU § C/2020/3300 (2020). ELI: <http://data.europa.eu/eli/reco/2020/518/oj>

Regulation (EU) 2016/679 of the European Parliament and of the Council 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, BOE § A-2020-3434 (2016). ELI: <http://data.europa.eu/eli/reg/2016/679/oj>

Terrón Santos, D. & Domínguez Álvarez, J.L. (2019). *Nueva regulación de la protección de datos y su perspectiva digital*. Granada, Spain: Comares.

Terrón Santos, D., Domínguez Álvarez, J.L. & Fernando Pablo, M.M. (2020). Los derechos fundamentales de la privacidad: derecho y necesidad en tiempos de crisis. *Revista General de Derecho Administrativo*, (55).

Troncoso Reigada, A. (2010). *La protección de datos personales: en busca del equilibrio*. Valencia, Spain: Tirant lo Blanch.

Velavan, T.P., & Meyer, C. G. (2020). The COVID-19 epidemic. *Tropical medicine & international health*, 25(3), 278. doi: [10.1111/tmi.13383](https://doi.org/10.1111/tmi.13383).

The necessary protection of special categories of personal data. A reflection on health-related data as an essential axiom to achieve the desired technological development in the face of COVID-19.

AUTHOR

José Luis Domínguez Álvarez

Young researcher of the Administrative Law Area of the University of Salamanca. Since the award of the Grant for the Training of University Faculty (FPU17/01088), and his subsequent incorporation to the University of Salamanca in 2018, he has focused his research activity on three priority lines of research: protection of personal data and information security, sustainable rural development and implementation of public policies of equality and fight against gender violence.

As a result of this, different publications on the new regulation on personal data protection, the modernisation and digitalisation of the Spanish public administration, the need to reformulate public policies for sustainable rural development or the importance of public policies in the promotion of gender equality stand out.

Orcid ID: <https://orcid.org/0000-0002-7623-8029>