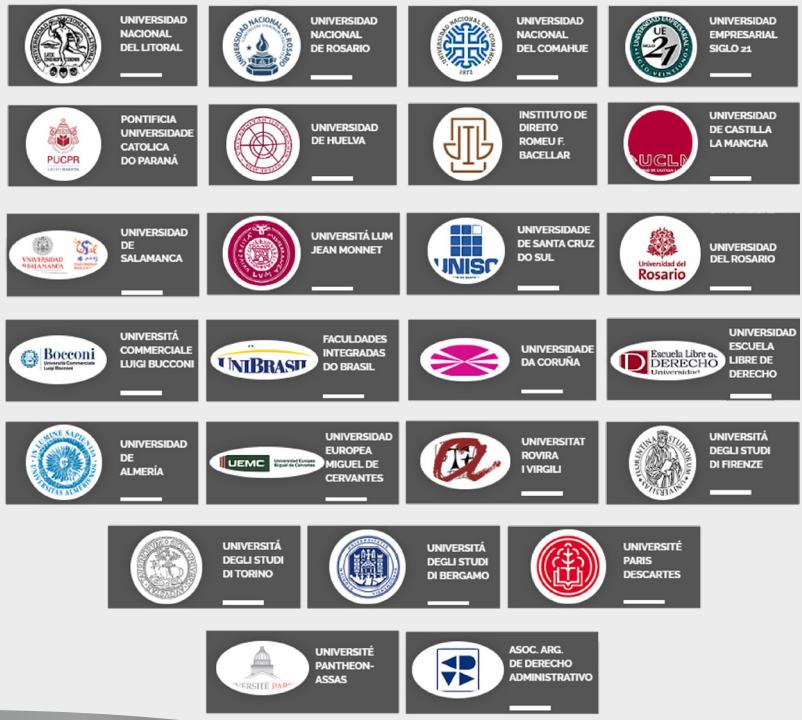
REVISTA EUROLATINOAMERICANA DE DERECHO ADMINISTRATIVO

VOL. 7 | N. 1 | ENERO/JUNIO 2020 | ISSN 2362-583X
SANTA FE | ARGENTINA | PERIODICIDAD SEMESTRAL

Revista oficial de la Red Docente Eurolatinoamericana de Derecho Administrativo
formada por las siguientes instituciones:



RED DOCENTE
EUROLATINOAMERICANA
DE DERECHO ADMINISTRATIVO

Licenciado bajo Licencia Creative Commons
Licensed under Creative Commons

DOI: 10.14409/redoeda.v7i2.9551

Revista Eurolatinoamericana de Derecho Administrativo

ISSN 2362-583X

Public administration's challenges in order to guarantee the fundamental right of personal data protection in the post-COVID-19 era*

Desafíos de las Administraciones Públicas para garantizar el derecho fundamental a la protección de datos personales en la era post-COVID-19

José Luis Domínguez Álvarez [I, **]

[I] Universidad de Salamanca (Salamanca, Spain)

jldoal@usal.es

https://orcid.org/0000-0002-7623-8029

Recibido el/Received: 30.08.2020 / August 30th, 2020
Aprobado el/Approved: 25.11.2020 / November 25th, 2020

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

Resumen:

La irrupción de la COVID-19 ha provocado una multitud de transformaciones de gran calado, que trascienden el ámbito puramente sanitario, dando lugar a importantes cambios socioeconómicos, entre los que destacan por su extraordinaria importancia la evolución de las formas tradicionales de intervención administrativa o la potenciación y/o aceleración de los avances derivados de la (re)volución digital. Así, en los últimos meses hemos asistido a la puesta en marcha de numerosas iniciativas destinadas a paliar los

Como citar este artículo | *How to cite this article*: DOMÍNGUEZ ÁLVAREZ, José Luis. Public administration's challenges in order to guarantee the fundamental right of personal data protection in the post-COVID-19 era. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 7, n. 1, p. 167-191, ene./jun. 2020. DOI 10.14409/redoeda.v7i2.9551.

*This contribution has been made under the Programme of Grants for University Teacher Training (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" of Salamanca University (GISALMAD-USAL).

** Researcher Staff (FPU17/01088) in Administrative Law Department of Salamanca University. PhD candidate in the Doctoral Program "Administration, Finance and Justice in the Social State" of Salamanca University. Specialized in the study of personal data protection in the digital revolution, the modernization of public administrations, sustainable rural development and emptied Spain, as well as the implementation of public policies on gender equality and the fight against gender violence. He was regarded with an Academic Excellence Prize in order to Salamanca University and an Academic Excellence Prize after finishing the Degree in Political Science and Public Administration with mention in Public Administration. He has written and published more than fifteen articles in prestigious Spanish academic magazines, numerous chapters in collective Academic Books and is the author of two full Books. E-mail: jldoal@usal.es.

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; apps; temperature; immunological passports.

efectos nocivos de la pandemia mediante el desarrollo de herramientas tecnológicas basadas en el tratamiento de categorías de datos personales especialmente protegidas, como los datos sanitarios, lo que plantea importantes cuestiones desde la perspectiva de la privacidad y los derechos digitales. El objetivo de este estudio es realizar un análisis detallado de algunos elementos esenciales, necesarios para lograr el difícil equilibrio entre la promoción de instrumentos tecnológicos que contribuyan a controlar los efectos de la COVID-19 aumentando los recursos disponibles para las autoridades sanitarias, y la salvaguarda del derecho fundamental a la protección de datos personales.

***Palabras clave**: COVID-19; protección de datos personales; privacidad; desarrollo tecnológico; autoridades sanitarias; apps; temperatura; pasaportes inmunológicos.*

Summary:

1. NEW TECHNOLOGIES AND THE MASS PROCESSING DATA AS SPEARHEAD OF THE HEALTH AUTHORITIES ACTIONS AIMED TO SLOWING DOWN THE EXPANSION OF COVID-19

On December 31st, 2019, appeared in Wuhan, China, a new outbreak of coronavirus, causing a huge commotion between the medical community and the rest of the world. This new coronavirus species was referred to as SARS-COV-2 (hereinafter COVID-19), causing a large number of infected people and deaths in China and outside it, becoming a global public health emergency[1].

[1] SARS-COV-2 is a virus with high homology with other pathogenic coronaviruses, such as those caused by zoonoses with bats causing approximately 646 deaths in China in the early 1990s. Its mortality rate is not so high (approximately 2-3%), but its rapid spread has led to the activation of protocols to stop its propagation. Despite the adoption of those measures and protocols, COVID-19 has become an unprecedented pandemic in our recent history, leading to the saturation of health resources and causing enormous human, economic and social losses. *Cfr.* CRUZ, Marcio, SANTOS, Edgar, VELÁZQUEZ, Manuel, y LEÓN, Moisés. COVID-19, una emergencia de salud pública mundial. **Revista Clínica Española**. 2020, p. 1.

The European continent, and especially Spain, haven't been oblivious to the devastating effects of the global pandemic[2], whose crudeness has been reflected in a huge amount of statistics that hide behind them a dramatic human, economic and social losses, wobbling the fundamental pillars on which the conception of modern State is based[3]. Every day, millions of citizens listen scared to the enumeration, by the health authorities and experts, of the increasing number of infections and deaths, bombed everyday by dire news, only broken by the hope of the gradual increase in the number of recovered sick people[4].

Given this difficult situation, the Government of Spain approved the adoption of the Royal Decree 463/2020 of March 14th declaring a State of Alarm[5] for the management of the health crisis caused by COVID-19, which provides of a series of immediate measures aimed to protect the health and safety of Spanish citizens, containing the progression of the disease and strengthening the public health system[6].

The severity and uniqueness of this measure allows us to affirm that the COVID-19 crisis confronts us nowadays with a multitude of unknown scenarios, and increases the

---

2 The World Health Organization raised the public health emergency caused by COVID-19 to an international pandemic on March 11th, 2020.

3 *Vid.* FERNÁNDEZ, Tomás Ramón. El Estado de Derecho, a prueba. In BLANQUER, David (Coord.). **COVID-19 y Derecho público (durante el estado de alarma y más allá**). 1st Edition. Valencia: Tirant lo Blanch, 2020, p. 19-20.

4 The case detection rate changes daily and can be followed virtually in real time on the following website provided by Johns Hopkins University. Available in: https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

5 It is necessary to point out that article 4, paragraph b), of Organic Law 4/1981, of June 1st, about the State of Alarm, Exception and Siege, allows the Government, in the exercise of the powers conferred by article 116.2 of the Constitution, to declare a State of Alarm, in all or in part of its territory in the event of a health crisis involving serious disturbances to normal health.

Regarding the State of Alarm, the Spanish Constitutional Court has had an occasion to pronounce itself in Order 7/2012 and Judgment 83/2016, in relation to the Royal Decree 1673/2010 (renew by the Royal Decree 1717/2010) which declared a State of Alarm for the normalization of air transport before the strike of the airport controllers. In these pronouncements, the Constitutional Court not only recognizes the normative character of the governmental decision declaring the State of Alarm, as it provides legality during its validity, but also states that, although it was formalized by a decree of the Ministers Council, it must be understood as it was a Parliamentary Act. *Vid.* LOZANO, Blanca. Análisis de urgencia de las medidas administrativas del estado de alarma. **Diario La Ley**, Madrid, n. 9601, p. 2-3, 2020.

In the words of the Spanish Constitutional Court, «aunque formalizada mediante decreto del Consejo de Ministros, la decisión de declarar el estado de alarma, dado su contenido normativo y efectos jurídicos, debe entenderse que queda configurada en nuestro ordenamiento como una decisión o disposición con rango o valor de ley. Y, en consecuencia, queda revestida de un valor normativo equiparable, por su contenido y efectos, al de las leyes y normas asimilables cuya aplicación puede excepcionar, suspender o modificar durante el estado de alarma» (STC 83/2016, FJ 10).

6 As PIÑAR, José Luis, recall «la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio regula en los artículos 4 a 12 el estado de alarma, que, según el art. 4, podrá ser decretado cuando, entre otras alteraciones graves de la normalidad, se produzcan "crisis sanitarias, tales como epidemias y situaciones de contaminación graves"». *Vid.* PIÑAR, José Luis. Transparencia y protección de datos en el estado de alarma y en la sociedad digital post COVID-19. In BLANQUER, David (Coord.). **COVID-19 y Derecho público (durante el estado de alarma y más allá**). 1st Edition. Valencia: Tirant lo Blanch, 2020, p. 136.

necessity of the whole global citizens to contribute, in the extent of its possibilities, to share the responsibility in order to overcome this difficult situation. In this sense, from Salamanca University we want to give our particular vision about the improvement of the clinical research processes that health authorities are trying to undertake, through the search for answers in the old, but, more than ever, needed State of Law in order to synchronize the fast technological development to the high guarantee levels needed for the protection of citizens fundamental rights and freedoms[7].

As is well known, digital technologies and data have a valuable role to play in the fight against the COVID-19 crisis[8]. These technologies and data provide, in many cases, an important tool to inform citizens and to assist public authorities in their efforts to contain the spread of the virus or to enable health organizations to exchange health data. However, as the European Commission has emphasized *«a fragmented and uncoordinated approach [to the use of new technologies based on the processing of personal data] jeopardizes the effectiveness of measures to combat the COVID-19 crisis, seriously damaging both the unified market and fundamental rights and freedoms»*[9].

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[10]. Animated by the multiple opportunities offered by these tools[11], including the possibility of providing guidance to citizens on measures such as social distancing, facilitating the organization of medical follow-up of patients, or tracing contacts, thereby limiting the spread of the disease and disrupting the transmission chains; the fact is, that combined with appropriate testing strategies and contact tracking, applications can be particularly important in providing information on the level of the circulation of the virus, assess the effectiveness of physical distance and lockdown measures, and guide the progressive lift of the lockdown measures to expedite, as much as possible, the daunting task that lies ahead us, the economic and social recovery. In this way, it is not difficult to find different public and private initiatives[12] aimed to create web applications and technological resources closely related to

---

7 *Vid.* TERRÓN, Daniel, DOMÍNGUEZ, José Luis, y FERNANDO, Marcos Matías. Los derechos fundamentales de la privacidad: derecho y necesidad en tiempos de crisis. **Revista General de Derecho Administrativo**, Madrid, n. 55, p. 1-31, 2020.

8 *Cfr.* MARTÍNEZ, Ricard. Covid-19 ¿hacia un rediseño de la privacidad?. **La Ley Privacidad**, Madrid, n. 5, 2020.

9 *Cfr.* COMMISSION RECOMMENDATION (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data.

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

11 *Cfr.* COTINO, Lorenzo. Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos. **IDP. Internet, Derecho y Política**, Barcelona, n. 31, pp. 1-17, 2020.

12 Following this trail of initiatives and movements in times of COVID-19, and taking into consideration the

the COVID-19 pandemic, initiatives that, in most cases, are based on the processing of health data, or what is the same, of specially protected personal data under 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 (General Data Protection Regulation–GDPR). Within these technological applications we find two large groups, depending on their purpose and typology: the alert and follow-up applications; and the self-diagnose and analysis of symptoms applications.

The first set of tools, the alert and monitoring applications, allow Member States to track contacts[13]. They may play an important role in the containment of the virus during the lift of the lockdown measures, scenario that health authorities will have to face once the contagion curve caused by COVID-19 falls down. Moreover, if it is a useful instrument for the public authorities, it can also become an important element to be considered by the citizens in order to maintain an effective and more selective social distance. In other words, the follow-up of the contacts implies that public health authorities can detect quickly all the contacts of a patient infected with COVID-19, ask them to practice self-isolation and, if they develop symptoms, test and isolate them quickly, reducing significantly the spread of the virus, and the devastating effects that came with it.

According to the criteria of the European Data Protection Board (EDPB), is in these type of applications that a special attention should be taken in order to minimize

processing of personal data and, in particular, the health-related data that many of these initiatives involve, the Spanish Data Protection Agency (SDPA) published a statement on 26 March on the criteria for making the use of these COVID-19 self-assessment apps and websites compatible with existing data protection regulations. According to the indications provided by the SDPA, «*únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia. Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados*». Official communiqué of the AEPD, retrieved from https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad.

[13] Oxford University researchers have highlighted the inability and ineffectiveness in the fight to control the spread of the pandemic through manual tracking of contagions, underlining the potential of using digital tracking applications that maximize citizen privacy: «*The newly emergent human virus SARS-CoV-2 is resulting in high fatality rates and incapacitated health systems. Preventing further transmission is a priority. We analyzed key parameters of epidemic spread to estimate the contribution of different transmission routes and determine requirements for case isolation and contact-tracing needed to stop the epidemic. We conclude that viral spread is too fast to be contained by manual contact tracing, but could be controlled if this process was faster, more efficient and happened at scale. A contact-tracing App which builds a memory of proximity contacts and immediately notifies contacts of positive cases can achieve epidemic control if used by enough people. By targeting recommendations to only those at risk, epidemics could be contained without need for mass quarantines ('lock-downs') that are harmful to society. We discuss the ethical requirements for an intervention of this kind*». *Vid.* FERRETTI, Luca, WYMANT, Chris, KENDALL, Michelle, ZHAO, Lele, NURTAY, Anel, ABELER, Lucie, PARKER, Michael, BONSALL, David, FRASER, Christophe. Quantifyng SARS-CoV-2 transmission suggest epidemic control with digital contact tracing. **Science**, Washington, vol. 368, n. 6491, p. 1, 2020.

privacy interferences allowing at the same time the required data processing with the aim to preserve public health. The EDPB points out the need to bet on the voluntary download of such applications, a choice that should be made by citizens as a sign of collective responsibility. This willingness is closely linked, as the European Commission itself has already pointed out in its recommendation, to the public's awareness of the trust and security resulting from the use of such tools, which illustrates the importance to respect data protection principles as a mechanism to increase the use from the public of these apps, maximizing their effectiveness[14].

In the second group of applications, we would find those aimed to self-diagnose and symptom analysis[15], which could provide relevant information on the number of cases with symptoms linked with COVID-19 by age and week, in well-defined areas where the application has high coverage[16]. If positive outcomes are obtained, national public health authorities may decide to use the application data results for surveillance in primary care in relation to COVID-19.

Regardless of the typology of the applications or tools to which we have referred, the truth 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 important benefits and represent an amazing opportunity to win the battle against COVID-19, as they not only improve the forecasting and decision-making capacity of health authorities, but also contribute to strengthen the effectiveness of social distance measures, thereby reducing significantly the spread of the pandemic, or by maximizing the always desired administrative efficiency, include in article 103.1 of Spanish Constitution, as a guiding principle for all the actions made by public administrations, that today, more than ever, is essential for the States when try to strategically allocate health resources in order to minimize the loss of human lives, which at this point is already unbearable.

---

14 *Cfr.* EUROPEAN DATA PROTECTION BOARD. **EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic**, Brussels, April 14, 2020, retrieved from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

15 Several Spanish Autonomous Communities have already developed their own tools for self-diagnose and symptom awareness. In the case of the Community of Madrid, this application is called CORONAMADRID, and in the case of the Community of Catalonia is called STOP COVID19 CAT. On the other hand, other autonomous communities have opted to enable tests with key questions about the causes of contagion and the mechanisms to protect themselves from the disease through their respective websites, such as Andalusia or Galicia. For its part, the Government of Spain has implemented a chatbot through the well-known messaging application WhatsApp, a tool that aims to guarantee attention to the citizen and not saturate lines of care or emergency (112), in the case of minor cases or mainly doubts.

16 As the European Union has pointed out in numerous position papers on this issue, the effectiveness of these mobile applications depends on a number of factors, including the percentage of the population using a mobile device and within that group, the percentage that has downloaded the application, that has given their consent to the processing of their personal data and has not withdrawn such consent.

However, the functions that the users have to enable in their smartphones in order to allow the use of the applications and tools described above, are likely to affect the exercise of certain fundamental rights[17] such as the right of private and family life, or the right of personal data protection[18], among others.

At this point, it's important to noted that the declaration of a State of Alarm does not entail the suspension of citizens fundamental rights and freedoms[19] beyond the regulations referred in article 11 of Organic Law 4/1981, of June 1st, about State of Alarm, Exception and Siege[20]. In no case, can rights be suspended, but only adopt limited and special measures that condition their exercise. This is the interpretation of article 55.1 of Spanish Constitution, which only allows the suspension of rights when a State of Exception or Siege is declared, but not the State of Alarm. And even then not all rights can be suspended, only those recognized in articles 17, 18, paragraphs 2 and 3, articles 19, 20, paragraphs 1.a), 1.d), and 5, articles 21, 28, paragraph 2, and article 37, paragraph 2, of Spanish Constitution. At this point it should be stressed

---

17 A good example of this scenario can be found in the mobile application, promoted by Beijing Government, known as «Health Code», tool that was distributed on popular platforms such as Alipay and WeChat to proceed to the collection of huge amounts of data relating to mobility and citizens health–far from the principles that should inform any processing of personal data in the European continent–. This tool allows to assign an identifying color to each person, depending on the data entered by the individual. This code (green, yellow or red) determines the mobility of the individual and may be required for verification by the authorities on public streets, at the entrances to commercial establishments, or in public transport. According to experts, eventhough this application has played a crucial role in significantly reducing the spread of the pandemic in the Giant Asian, has implied giving up the privacy of its society as a whole, an extremely dangerous situation in the turbulent waters of the digitalization and datafication world. *Cfr.* MOZUR, Paul, ZHONG, Raymond, KROLIK, Aaron. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. **New York Times**, New York, march, 2020. Retrieved from www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

18 In this sense, leading academics, experts in the field of privacy, point out that *«la pandemia provocada por el patógeno COVID-19 ha puesto sobre la mesa las virtudes y carencias del modelo europeo de protección de datos personales. Este modelo se caracteriza por ofrecer un marco altamente tuitivo en la garantía del derecho fundamental a la protección de datos, particularmente funcional para la garantía de este derecho, pero también por un planteamiento proactivo que implica un compromiso de responsables y encargados en la garantía del derecho fundamental. Este modelo aporta sin duda enormes ventajas desde el punto de vista de la garantía de nuestras libertades en una sociedad democrática. Pero no está exento de inconvenientes cuando su aplicación no se modula desde un enfoque funcional. Y la crisis de COVID-19 ha puesto de manifiesto la existencia de enfoques puramente reactivos, centrados exclusivamente en un enfoque desde el Reglamento General de Protección de Datos, con una interpretación del entero ordenamiento jurídico a la luz del derecho a la protección de datos». Vid.* MARTÍNEZ, Ricard. Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. **Diario La Ley**, Madrid, n. 9601, p.1, 2020.

19 *Vid. op. cit.* PIÑAR, José Luis. Transparencia y protección…, p. 136-137.

20 In this sense, the precept establishes that *«el decreto de declaración del estado de alarma, o los sucesivos que durante su vigencia se dicten, podrán acordar las medidas siguientes: a) Limitar la circulación o permanencia de personas o vehículos en horas y lugares determinados, o condicionarlas al cumplimiento de ciertos requisitos. b) Practicar requisas temporales de todo tipo de bienes e imponer prestaciones personales obligatorias. c) Intervenir y ocupar transitoriamente industrias, fábricas, talleres, explotaciones o locales de cualquier naturaleza, con excepción de domicilios privados, dando cuenta de ello a los Ministerios interesados. d) Limitar o racionar el uso de servicios o el consumo de artículos de primera necesidad. e) Impartir las órdenes necesarias para asegurar el abastecimiento de los mercados y el funcionamiento de los servicios de los centros de producción afectados por el apartado d) del artículo cuarto»*.

that the right of personal data protection is an autonomous right[21] which is based on article 18.4 of Spanish Constitution, there so cannot be suspended even in States of Exception and Siege, much less in a State of Alarm.

This means, as the Spanish Data Protection Agency (SDPA) has rightly pointed out on several occasions[22], that the rules on personal data protection, which main purpose is none other than safeguard the legal protection of a fundamental right, apply in their all integrity to all the situations arising processing of personal data related to the propagation of COVID-19, since there is no legal reason to suspend fundamental rights, nor has such a measure been adopted.

However, without prejudice the foregoing ideas that we just point out, it should be noted that the regulations about personal data protection, such as the European General Data Protection Regulation (GDPR) and the Organic Law 3/2018 of 5 December, on Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), contain the necessary safeguards and rules to legitimately allow the processing of personal data in situations, such as the present one, where there is a general health emergency. Therefore, in the application of those safeguards and rules provided for these emergency cases by the legislation on protection of personal data, in line with the sectoral regulations applicable in the field of public health, data protection considerations, within the limits provided for by law, should not be used as an obstacle or as a limit to the effectiveness of the measures taken by authorities, especially health authorities, in the fight against the pandemic, since the legislation on protection of personal data already contains regulations for such cases that harmonize and balance the public health interest and the protection of those fundamental rights in order to achieve a common good.

Therefore, it should be understood that the protection of personal data is not intended to obstruct the processing of necessary personal data for the adoption of effective measures against COVID-19, but quite the contrary, the aim is to achieve a correct application of the regulation of a fundamental right, the personal data protection,

---

[21] The Spanish Constitutional Court has specifically defined the right of personal data protection as an autonomous right in its Judgment 292/2000 of 30 November as follows: *«el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos». Cfr.* Judgment 292/2000, of 30 November, FJ. 7.

[22] It is necessary to highlight the clarifying Report 0017/2020 of the Spanish Data Protection Agency, in relation to the processing of data resulting from the current situation resulting from the spread of the COVID-19 virus. Retrieved from: https://www.aepd.es/es/documento/2020-0017.pdf.

which is the basic institute for the full effectiveness and guarantee of all fundamental rights constitutionally recognized, standing as one of the foundations of the Social and Democratic State of Law, especially in the digital (re)volution era that we live on.

It is not intended to create obstacles by making the personal data protection an immovable barrier, as some academics have pointed out, but rather strengthen the normal application of the old State of Law. In this sense, the words of the Spanish academic José Luis PIÑAR MAÑAS – expert in the field of personal data protection regulations and whose actions as Director of the SDPA have left an profound mark in the development of privacy in our legal system – are comforting, noting that «the situation of exceptionality does not allow an exceptional application or even non-application of the Law, but the most normal of its applications»[23].

In this regard, as will be analyzed below, the treatments referred in Order SND/297/2020 of 27 March must be based on an enabling title that makes them lawful, title that can certainly be found in article 6.1.d) and e) and in several paragraphs of article 9.2, both of the European GDPR, and those data treatments must respect the specific principles of personal data protection, such as, purpose, security, minimization of data and limitation of the conservation period. And in particular the principle of proactive accountability, the cornerstone of the new data protection regulation[24], which demands and requires that data protection must be taken into account by default and since the beginning of the design – which is particularly important when it comes to developing applications or technological tools to support the management of the health crisis –, carrying out a data protection impact assessment as the conditions laid down in article 35 of the European GDPR are undoubtedly there, and the adoption of a register of all the processing activities in accordance with article 30 of the European GDPR, which must also be public, according to art. 31.2 LOPDGDD.

In addition, it is essential to inform all interested parties as its demanded in articles 13 and 14 of the European GDPR unless it is established that some of the circumstances provided for in paragraphs 4 and 5 respectively of both articles exist. Similarly, the requirements stablished by the Royal Decree-Law 14/2019, of 31 October, on digital administration, public sector procurement and telecommunications should be applied[25].

---

[23] *Vid.* PIÑAR, José Luis. Privacidad en estado de alarma y normal aplicación de la Ley. **Hay Derecho**, **Expansión**, Madrid, abril, 2020. Retrieved from: https://hayderecho.expansion.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/.

[24] *Vid.* TERRÓN, Daniel, DOMÍNGUEZ, José Luis. **Nueva regulación de la protección de datos y su perspectiva digital**. 1st Edition. Granada: Comares, 2019, p. 14.

[25] *Vid.* PIÑAR, José Luis. 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**, Madrid, n. 3, 2020; DOMÍNGUEZ, José Luis. Comentario al Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Un paso más hacia la configuración de una regulación efectiva del ciberespacio. **AIS: Ars Iuris Salmanticensis**, Salamanca, vol. 8, n. 1, p. 217-223, 2020.

These same ideas that we are now enunciating are taken up in the same way by the European Data Protection Supervisor (EDPS) in its latest positions[26].

Precisely in the spirit of unite the technological development as a tool to combat the advancement of the propagation of COVID-19 virus, with high privacy standards, the European Union has recently created the Pan-European Privacy-Preserving Proximity Tracing [27] (PEPP-PT), a project which aims to provide a single, open source solution for collecting mobile data in the countries of the European Union, with strict respect for European legislation and principles of privacy and protection of personal data.

With this technology project, the European Union is taking a giant step forward in the fight against the propagation of COVID-19 virus, strengthening interoperability between countries, guaranteeing greater traceability to ensure the exchange of anonymous data in relation to the pandemic between Member States and advance in the adoption of a pan-European approach to the use of mobile applications, in order to empower citizens to take effective and more targeted social distancing measures, as well as to alert, prevent and monitor contacts with the only aim of limiting the spread of COVID-19 disease.

2. THE TREATMENT OF SPECIAL CATEGORIES OF PERSONAL DATA IN TIMES OF CRISIS: LEGAL REGIME OF HEALTH DATA

As has been shown, the declaration in Spain of the State of Alarm after the adoption of the Royal Decree 463/2020, of 14 March, does not allow to limit fundamental rights and freedoms[28] beyond what is provided for in article 11 of Organic Law 4/1981, which

---

[26] In response to a consult made from the Director-General of the European Commission's Directorate-General for Communications, Networks, Content and Technology Roberto Viola, the current European Data Protection Supervisor (EDPS), Wojciech Rafał Wiewiórowski, published on 25 March 2020, a letter, giving his opinion on the possibility of using the traffic data of the population's mobile devices as a source for monitor people as a measure against the current pandemic expansion. Thus, the EDPS notes the following: «*Firstly, let me underline that data protection rules1 currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics. I am aware of the discussions taking place in some Member States with telecommunications providers with the objective of using such data to track the spread of the COVID-19 outbreak. I share and support your call for an urgent establishment of a coordinated European approach to handle the emergency in the most efficient, effective and compliant way possible. There is a clear need to act at the European level now. On the basis of the information provided in your letter and in absence of a more specific data model, please find below some elements for your consideration*». Retrieved from: https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.

[27] Spain joined the consortium of Pan-European Proximity Tracking to Preserve Privacy on 13 April 2020, through the Secretary of State for Digitization and Artificial Intelligence (AI). The consortium has more than 130 members from eight European countries (Spain, Germany, France, Italy, Switzerland, Belgium, Denmark and Austria), including scientists, technologists and experts from renowned international research and business institutions.

[28] *Cfr.* FERNÁNDEZ DE GATTA, Dionisio. Los problemas de las medidas jurídicas contra el coronavirus: las dudas constitucionales sobre el Estado de Alarma y los excesos normativos. **Diario La Ley,** Madrid, n. 9634, p. 1-21, 2020; FERNÁNDEZ DE GATTA, Dionisio. El estado de alarma por la epidemia del coronavirus y sus problemas constitucionales legales. **AIS: Ars Iuris Salmanticensis**, Salamanca, vol. 8, n.1, p. 27-40, 2020.

has a number of limitations for the public authorities from the point of view of the protection of personal data.

In general, the European Data Protection Board[29] like various European supervisory authorities[30], including the SDPA, have made public statements regarding the processing of personal data in the context of the COVID-19 crisis. All these statements express a common feeling, stressing that the regulations on data protection, and in particular the European GDPR, do not prevent taking measures in the fight against the coronavirus pandemic, but warn that even in these exceptional circumstances those who personal data process measures must ensure their protection, more if we take into account that in many cases such process use particularly sensitive data, such as health-related data.

Under the current regulations, health data represent what are known as special categories of personal data. As MEDINA GUERRERO rightly points out, the European General Data Protection Regulation qualifies such data telling that «by their nature, are particularly sensitive in relation to fundamental rights and freedoms» (Whereas 51 GDPR). And, the first paragraph of article 9 of the European GDPR essentially contains the data which were already considered to merit greater protection in article 8 of Directive 95/46/EC: ethnic or racial origin; political opinions; religious or philosophical

---

29 And thus, the European Data Protection Board 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 regulations on protection to proceed to the fight against the coronavirus pandemic, noting 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*».

30 In front of those who express their disagreement with the actions of the control authorities, demonizing their diligent work, we can only show our deepest disagreement. Let us remember that these types of institutions, among which the Spanish Data Protection Agency stands out, embody the «principle of independent control» in other words, they are a prerequisite for considering that the right to data protection is sufficiently guaranteed. Thus, it is presumed that, in the absence of such authority, the legal framework surrounding the right of personal data protection can in no way be considered acceptable. *Cfr.* PIÑAR, José Luis. El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. **Asamblea. Revista Parlamentaria de la Asamblea de Madrid**, Madrid, n. 13, p. 24, 2005.

convictions; trade union membership; health and sexuality, although as far as the last one is concerned now it refers to: «data relating to sexual life or sexual orientations»[31].

For its part, article 4.15) of the European GDPR specifies and clarifies the concept of «health data» as opposed to Directive 95/46/EC, which did not address its conceptualization. According to that particular article, health data means «personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status».

In this context, it is necessary to clarify the legal regime and the possibilities of the processing of the health data, which, as we have revealed, are essential to promote a necessary and adequate technological development to win over COVID-19.

In this sense, the first thing we have to point out is that the European GDPR itself, in whereas 46, recognizes that, in exceptional situations, such as the one we are living at the moment, the legal basis for treatment may be multiple, based both on the public interest, as in the vital interest of the data subject or other person.

> *(46) «The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters».*

Therefore, as a legal basis for a lawful process of personal data[32] – without prejudice to other ones, such as the fulfilment of a legal obligation ex article 6.1.c) of the European GDPR, situation that can occur in those actions of treatment personal data developed by the employer in the prevention of occupational risks of its employees –, the GDPR explicitly recognizes two that legitimize the treatment of differentiated personal data: when the processing is necessary to protect the vital interests of the data subject or another natural person – article 6.1.d) –, and when the processing is necessary for

---

31 *Vid.* MEDINA, Manuel. Categorías especiales de datos. In RALLO, Artemi (Dir.). **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**. 1st Edition. Valencia: Tirant lo Blanch, 2019, p. 251.

32 Article 5 of the European GDPR sets out the principles to which the processing of personal data must be subject, as stated by PUYOL *MONTERO «por un conjunto de reglas que determinan cómo se deben recoger, tratar y ceder los datos de carácter personal, a los efectos de garantizar la intimidad y demás derechos fundamentales de los titulares de los datos, los consumidores y usuarios, y en definitiva los ciudadanos». Vid.* PUYOL, Javier. Los principios del derecho a la protección de datos. In PIÑAR, José Luis (Dir.). **Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad**. 1st Edition. Madrid: Editorial Reus, 2016, p. 135-150.

the accomplishment of a mission carried out in the public interest or in the exercise of public powers conferred to a specific institution – article 6.1.e).

Article 6.1.d) of the European GDPR considers not only that the vital interest is a appropriate legal base for data treatment in order to protect the data subject, but that legal base can also be used to protect the vital interest «of another natural person», which by extension means that such natural persons may even be unidentified or unidentifiable; in other words, that legal base for the data treatment – the vital interest –, may be enough for the processing of personal data aimed to protect all those persons susceptible to be infected in the spread of an epidemic or a pandemic, which would justify, from the point of view of the processing of personal data, as broadly as possible, the measures taken to that porpoise, even if they are aimed to protect unnamed or unidentified or unidentifiable persons, because the vital interests of such natural persons must be safeguarded, and this is recognized by the rules on the protection of personal data[33].

In accordance with the previous words, it does not seem strange that this legal basis of treatment of personal data[34], has traditionally been linked to the one stablished in article 9.2 c) of the European GDPR, as it allows to lift the prohibition on the processing of 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, where the person concerned is not physically or legally capable of giving his or her consent[35].

However, for the processing of health-related data the legal base stablished by article 6 of the European GDPR is not enough, in accordance with article 9.1 and 9.2 of the European GDPR it must necessarily exists an extraordinary circumstance that allow to lift the prohibition on the processing of that special category of data.

---

[33] On this issue, the AEPD in its Legal Report 0017/2020 states that *«el apartado 3 del artículo 6 RGPD no establece la necesidad de que la base del tratamiento por razón de interés vital haya de ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros aplicables al responsable del tratamiento, pues dicho apartado se refiere exclusivamente a los tratamientos establecidos para el cumplimiento de una obligación legal, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, ambas referidas en las letras c) y e) de dicho artículo 6 RGPD, pero no para los tratamientos incluidos en la letra d)». Cfr.* SPANISH DATA PROTECTION AGENCY. **Legal Report 0017/2020**, Madrid, p. 2, 2020. Retrieved from: https://www.aepd.es/es/documento/2020-0017.pdf.

[34] In this regard, the Group of article 29 in its Opinion 6/2014 considered: *«(…) que debe hacerse una interpretación restrictiva de esta disposición, respetando el espíritu del artículo 8. Aunque el artículo 7, letra d), no limita específicamente el uso de este fundamento jurídico a situaciones en las que el consentimiento no puede utilizarse como fundamento jurídico por los motivos especificados en el artículo 8, apartado 2, letra c), es razonable suponer que en situaciones en las que exista la posibilidad y la necesidad de solicitar un consentimiento válido, el consentimiento deberá, por supuesto, solicitarse siempre que sea posible. Esto también limitaría la aplicación de esta disposición a un análisis caso por caso y no puede normalmente utilizarse para legitimar cualquier recopilación o tratamiento masivos de datos personales. En caso de que esto resultara necesario, las letras c) o e) del artículo 7 serían motivos de legitimación más apropiados para el tratamiento»*.

[35] *Vid.* PUENTE, Agustín. Principios y licitud del tratamiento. In RALLO, Artemi (Dir.). **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**. 1st Edition. Valencia: Tirant lo Blanch, p. 115-168, 2019.

In the specific scenario in which we find ourselves, this circumstance should be found in several of the sections of article 9.2 of the European GDPR. So, the prohibition on the processing of health-related personal data will not apply in the following cases:

First, in accordance with point b) of that article when processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

Second, in accordance with article 9.2.g) of the European GDPR, when processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Third, under point i), when processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

Fourth, and in accordance with the precept of the letter h), when processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 of the same article which refers to when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

To these exceptions, the SDPA considers its necessary to add a fifth and final closure circumstance that would allow the processing of health-related data in times of health crisis. In this way, according to the Agency's criteria *«it could apply the circumstance established in letter c) of article 9.2, when processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent»*[36].

[36] *Vid. op. cit.* SPANISH DATA PROTECTION AGENCY. **Legal Report 0017/2020**…, p. 4.

Consequently, in a health emergency such as this one we are experiencing right now, it should be borne in mind that – within the exclusive scope of the rules of personal data protection –, the application of personal data protection rules will enable the «controller» of the data treatment to take the necessary decisions 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, only and just only, when the essential content of the personal data protection right is respected and the appropriate and specific measures are put in place[37] in order to protect the interests and fundamental rights of the data subject.

In this regard, the data controllers, in order to ensure their correct performance and to effectively safeguard the vital interests of the citizens, must act in accordance with the instructions provided by the health authorities, in accordance with the sectoral regulatory rules set to that effect.

It should be pointed out that, the Spanish legal system establishes a series of legal, necessary and adequate rules to deal with situations of health risk such as the scenario caused by the irruption of the COVID-19 virus. We are referring, as it could not be otherwise, to the Organic Law 3/1986, 14 of April, about Special Measures in Public Health (changed through the Royal Decree 6/2020, 10 of 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 to the State Law 33/2011, 4 of October, Public Health General Act (LGSP).

In this regard, article 3 of Organic Law 3/1986, provides that:

> *«in order to control contagious diseases, the health authority may, in addition to carrying out general preventive actions, take appropriate measures for the control of patients, of persons who are or have been in contact with them and of the immediate environment, as well as those deemed necessary in the event of a transmissible risk».*

For its part, article 54.1 of LGSP establishes the following:

> *«without prejudice to the measures provided for in Organic Law 3/1986 of 14 April on Special Measures in the Field of Public Health, on an exceptional basis and when reasons of extraordinary gravity or urgency so require, the General Administration of the State*

[37] Taking into account the principle of proactive responsibility – article 5.2 GDPR –, and the principles of data protection by default and form the beginning of the desing – article 25 GDPR –, appropriate technical and organizational measures, such as pseudonymization, and even aggregation and anonymization of health-related data, should be adopted both at the time of determining the means of treatment and at the time of the processing itself. In addition, in accordance with the principle of data minimization – article 5.1.c) GDPR –, it must be ensured that, by default, only the necessary personal data for each of the specific purposes of the processing are processed and will not be accessible, without the consent of the person, to an indeterminate number of persons.

and those of the Autonomous Communities and cities of Ceuta and Melilla, within the scope of their respective competences, may take all measures necessary to ensure compliance with the law».

Therefore, when we deal with contagious diseases, the sectoral health legislation referred to above, gives the health authorities the necessary powers to put in place the necessary measures – provided for in those laws – where urgent or necessary health reasons are required.

Consequently, from the point of view of the processing of personal data, the protection of essential interests in the field of public health is a responsibility of the health authorities from the public administrations, who might take the necessary measures to safeguard those essential public interests in situations of public health emergency. These measures include those related to the processing of personal data, for which the collaboration with the Spanish Data Protection Agency should be strengthened, as an institution which must be given an extraordinary role in ensuring that personal data are properly processed, respecting both the rights of all citizens and the full compliance of the legislation on the protection of personal data.

In this way, the same health authorities will be responsible for ensuring the proper processing of personal data, in accordance with the requirements and obligations set out in the legislation on the protection of personal data. Especially regarding the strict compliance of the principles set forth in article 5 of the European GDPR, including the principle of lawful, fair and transparent processing of personal data, purpose limitation (in this case, safeguarding the vital/essential interests of natural persons), the principle of accuracy, and, of course, and this should be emphasized, the principle of data minimization, the importance of which has already been referenced, ensuring that the data processed will be exclusively those necessary for the intended purpose, without the possibility of extending such processing to any other personal data not strictly necessary for that purpose, in this case convenience cannot be confused with necessity, because the fundamental right to data protection continues to apply normally[38], without prejudice to the fact that, as stated above, the personal data protection rules themselves provide that in emergency situations, for the protection of essential public health and/or vital interests of natural persons, the necessary health data to prevent the spread of the disease causing the health emergency may be processed[39].

---

[38] The development of technological applications aimed to combat the spread of the pandemic caused by COVID-19 must be done in a responsible manner, documenting with a data protection impact assessment all privacy implemented by design a privacy by default mechanisms, and the source code must be publicly available for the widest possible scrutiny by the scientific community. *Cfr. op. cit.* EUROPEAN DATA PROTECTION BOARD. **EDPB Letter concerning**…, p.1-4.

[39] *Vid. op. cit.* SPANISH DATA PROTECTION AGENCY. **Legal Report 0017/2020**…, p. 7.

3. THE NEW CHALLENGES FOR PUBLIC ADMINISTRATIONS TO ENSURE PRIVACY IN THE POST-COVID-19 SCENARIO

As we have pointed out above, many efforts have been made by public administrations in recent months to seek innovative solutions to contribute to increase the resources available to the public health system and, on the other hand, to try to control the huge and rapid expansion of the pandemic, which far from diminishing as the lockdown measures start lo lift up, threatens to cause a second, bloodier wave of infection than the previous one. In this context, where there is a widespread expansion of various actions based on the processing of health data, practices which in many cases are difficult to integrate into a strategy of realistic, effective, scientifically based, legitimate, legally and organizationally proportionate measures, which may lead to situations of loss of freedoms, discrimination, or other damage to the personal status of citizens.

In this difficult situation, public administrations and especially the health authorities, have to maximize efforts to ensure an effective legal protection of the personal data as an indispensable condition for guaranteeing the fundamental rights and freedoms of citizens in the digital (re)volution era. If, on the contrary, the public authorities respond to this crucial issue with passivity and lack of diligence, they will contribute to further stirring up the storm caused by the irruption of COVID-19, thus contributing to the erosion and weakening of the European model of privacy, the creation and establishment of new forms of discrimination and social inequality this time based on purely health reasons, and the deterioration, ultimately, of the institutions of the Social and Democratic State of Law itself, effects, all of them, very difficult to restore.

3.1. Temperature screening

As it has already been pointed out in this paper, the gradual lift of the lockdown and social distancing measures – that also provoked a limitation of economic activity –, aimed to achieved the so-called «new normality» is determining the implementation of measures aimed to prevent the expansion of the COVID-19 virus. These measures include, across the board and apparently in a wide variety of settings, the screening of people's temperature to determine the possibility or not of their access to workplaces, shops, educational establishments or other types of facilities, which are being carried out without the prior and necessary criteria of the health authorities[40].

[40] *Vid.* SPANISH DATA PROTECTION AGENCY. **Comunicado en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos**, Madrid, 2020. Retrieved from: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos.

Firstly, it is necessary to clarify that, when we talk about actions[41] based on screening citizens temperature, we are referring to a set of operations involving the processing of personal data which, as such, must be adjusted to the legal requirements of the personal data protection laws that we already point out before. In this regard, it should be recalled that the rules on the protection of personal data, far from represent a barrier or an obstacle to the development of tools and techniques that help us mitigate the effects of this health crisis, contains specific conditions that allows covering situations of health emergency such as the current one, while allowing the continuous application of the principles and guarantees that protect the fundamental right of personal data protection.

In addition, it should be pointed out that this temperature screening procedure involves a particularly intense interference with some fundamental rights of affected people. In one hand, because it involves data related to individuals health, or what is the same, to special categories of personal data, because the body temperature of a person is a health data itself, from which it can be inferred that a person has or does not have a certain disease, as occurs in the case of COVID-19.

Another of the worrying extremes arising from the application of this type of techniques in order to detect and control the health crisis – beyond the fact that on many occasions its implementation is undertaken without the prior determination of the competent health authorities –, is the lack of precision about the necessity and suitability of these devices for the purpose and effectiveness on the prevention of the spread of the, avoiding the necessary regulation about the limits and the specific guarantees of the processing of the personal data of those concerned.

In this regard, it should be borne in mind – among other things – that according to the information provided by the health authorities, there is a percentage of people infected asymptomatically[42], where there is no fever. More so, fever is not always one of the main symptoms present in symptomatic patients, in particular in the early stages of the development of the disease, and on the other hand, there are people that may have high temperatures and fever due to other causes than the COVID-19 virus that will be victims of discrimination and lockdown measures[43].

---

41 Especially relevant is the existing debate about the application of video surveillance cameras that include the ability to take the temperature to individuals crossing a certain area, without requiring in many cases any action on their part. These cameras identify human faces by means of artificial intelligence algorithms, discriminate them from the rest of the elements that appear in the image and reveal the approximate body temperature of each individual.

42 *Vid.* NISHIURA, Hiroshi, KOBAYASHI, Tetsuro, MIYAMA, Takeshi, SUZUKI, Ayako, JUNG, Sung-mok, HAYASHI, Katsuma, KINOSHITA, Ryo, YANG, Yichi, BAOYIN, Yuan, AKHMETZHANOV, Andrei, LINTON, Natalie. Estimation of the asymptomatic ratio of novel coronavirus infections (COVID-19). **International journal of infectious diseases**, n. 94, p. 154, 2020.

43 It should be remembered that fever is one of the most probable clinical evidence associated with a symptomatic COVID-19 infected, but it should also be considered that there is a high percentage of asymptomatic infected

For all these reasons, the SDPA rightly considers that «*these measures should be applied only on the basis of the criteria defined by the health authorities, both as regards their usefulness and their proportionality, that is to say, to what extent this usefulness is sufficient to justify the sacrifice of the individual rights that the measures entail and to what extent these measures could or could not be replaced, equally effectively, by less intrusive measures*»[44].

This is why it is urgent that health authorities pay a closer attention to the proliferation of this type of techniques that have been performed without the required legal and administrative guarantees[45], as they represent a high threaten to privacy and introduce us to new risks from the perspective of equality, as they encourage the emergence of new forms of discrimination because health reasons; at the same time as they lack the necessary effectiveness to ensure the proper protection of public health.

3.2. Teleworking and information security

One of the most obvious consequences of the irruption of the COVID-19 health crisis has been the generalization of teleworking and the acceleration and implementation of the processes of digitalization of society. However, the introduction of teleworking has many implications for information security and the protection of personal data[46].

Mindful of the critical importance of this issue in ensuring the survivance of the State, the continuity of business processes, and the rights and freedoms of data subjects whose data are being processed, several institutions have taken advantage of the situation to produce a series of documents and reports aimed to combat cyber threats and attacks and to maximize security information in teleworking situations.

The National Cryptological Spanish Centre (INCIBE), through the Internet User Security Office (OSI), establishes a series of priority actions to be developed with the aim to strengthen cybersecurity and minimize the risks involved in boosting telework. These measures include some destined to ensure the proper functioning of the devices used

---

people, and that high temperature may be associated with other pathologies. Apply these measures without a criterion set by the health authorities as to what fever value is significant, on which other symptoms need to be checked, with handling that may lack sufficient precision in the hands of unqualified personnel, the use of these systems could create a false sense of security that facilitates contact with genuinely infected persons. *Vid.* QIU, Haiyan, WU, Junhua, HONG, Liang, LUO, Yunling, SONG, Qifa, CHEN, Dong. Clinical and epidemiological features of 36 children with coronavirus disease 2019 (COVID-19) in Zhejiang, China: an observational cohort study. **The Lancet Infectious Diseases,** London, vol. 20, p. 689-696, 2020.

44 *Vid.* SPANISH DATA PROTECTION AGENCY. **Comunicado en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos**, Madrid, 2020. Retrieved from: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

45 During the first three months of the health crisis alone, the Spanish Agency for Data Protection has received a total of 86 complaints related, fundamentally, to the communication of data on the affectation or not by COVID-19 in the workplace or by the temperature screening in that environment.

46 *Vid. op. cit.* PIÑAR, José Luis. Transparencia y protección…, p. 166.

to carry out teleworking, some destined to safeguard the integrity of the information of organizations, and some aimed to ensure the security of the connection networks[47].

Similarly, the National Cryptological Spanish Centre prepared the report CCN-CERT BP/18, under the tittle "*Safety recommendations for teleworking situations and surveillance reinforcement*", in order to facilitate some guidelines to ensure the security of all tools and solutions used in teleworking and thus to continue to maintain the confidentiality, integrity and availability of information, as if in the office[48].

For its part, the Spanish Data Protection Agency has presented a set of recommendations addressed both to the controllers of personal data and to the employees involved in the development of activities of processing such data in situation of teleworking, all of these in order to minimize the risks on citizens privacy. Among the recommendations addressed to employers are the following: restriction of access to information, periodic configuration of equipment and devices used in mobility situations, monitoring of the accesses to the corporate network from the outside, and the rational management of data protection and security. The guidelines provided to employees include the respect of information protection policy in situations of mobility defined by the controller, the protection of the device used in mobility and the access to it, ensuring the protection of the information being handled, the storage of the information in the network spaces enabled for this purpose, and the immediate communication of any security breach that may occur[49].

3.3. Immunological passports and Immunological curriculum vitae

The possibility of promoting the use of digital applications and tools equivalent to what would be a passport or safe conduct on paper, by assigning color codes or QR codes to identify «healthy» people from «sick» people, is currently under international discussion, because the use of these measures to identify the degree of immunity of COVID-19 presented by the holder of the device, which will be the factor determining the freedom of movement of the its holder and his or her ability to access certain

---

47 Information available in: https://www.osi.es/es/cibercovid19.

48 *Vid.* CENTRO CRIPTOLÓGICO NACIONAL. **Informe BP/18. Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia,** Madrid, 2020. Recovered from: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html.

49 *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo,** Madrid, 2020, p. 1-6. Recovered from: https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf.

establishments[50]. This possibility, to which Spain is not a stranger[51], is an alternative to ease mobility restrictions for infected people who have successfully overcome the disease, allowing for the recovery of productive activities and accelerating socio-economic reconstruction efforts. However, this initiative raises several worrying ethical and legal questions that transcend the privacy sphere[52].

In the first place, the implementation of this immunity passport represents an interference with citizens right to privacy, as it incorporates sensitive data, such as any data relating to health.

Beyond the difficult legal context that this measure could have from the perspective of the regulation of personal data, the initiative also presents important gaps from the perspective of effectiveness, in addition to having significant ethical connotations.

Regarding the first of the issues, it is necessary to stress that, even today, the scientific community has innumerable doubts about the essential aspects of immunity acquired after overcoming the infection caused by COVID-19 virus[53].

On the other hand, as far as ethical aspects are concerned, it should be pointed out that not so well taught public policies on immunity passports can cause serious damages not initially anticipated, such as the establishment of higher levels of inequality and discrimination, the emergence of new sources of stigmatization of certain sectors of society and the increase in risks and unequal treatment[54] of individuals due to erroneous test results for COVID-19 virus[55].

These are some of the reasons that justify the majority rejection of the academic sector and health authorities on this type of immunological passports, an initiative that presents more shadows than lights, and which constitutes an additional concern to be taken into account by data protection supervisory authorities.

---

50 *Vid.* SPANISH DATA PROTECTION AGENCY. **El uso de las tecnologías en la lucha contra el COVID19,** Madrid, 2020, p. 10.

51 Some of the Autonomous Communities most affected by the COVID-19 pandemic, as in the case of the Community of Madrid or Castilla and León, have repeatedly expressed their intention to implement this type of immunological passports, despite the contrary recommendations of the Spanish Data Protection Agency, the Ministry of Health and the opinion of renowned academics in the field.

52 *Vid.* SALAS, Sofía. Consideraciones éticas respecto del "pasaporte" COVID-19. **Revista chilena de infectología**, Santiago de Chile, vol. 37, n. 3, p. 329-330, 2020.

53 It should be recalled that in August 2020 the first cases of reinfection by SARS-COV-2 were officially recorded, which makes it possible to seriously question both the purpose and the effectiveness of the actions aimed at the establishment of immunological passports.

54 Immunological passports have not taken long to move into the workplace, which has led to the inclusion of information on their health in the selection criteria of certain business entities.

55 *Vid.* VOO, Teck Chuan, CLAPHAM, Hannah, TAM, Clarence. Ethical Implementation of Immunity Passports During the COVID-19 Pandemic. **The Journal of infectious diseases**, Oxford, vol. 222, n. 5, p. 715-718, 2020.

4. CONCLUSIONS

The fast technological development presents itself today as a powerful tool, capable of contributing significantly in the complex decision-making processes of the health authorities aimed to overcome the global «alarm» situation caused by COVID-19 virus, a pandemic which has caused devastating effects, leaving behind a painful trail of human lives and socio-economic losses, and which has hit the pillars of the European Union, even calling into question the very values inherent in the concept of European citizenship.

But beyond these visible devastating effects, COVID-19 has raised important unknowns questions that have led to the creation of important academic discussions in which, on many occasions, the validation and effectiveness of the existing model of fundamental rights and freedoms has come into play. An example of these fierce debates is the virulent confrontation that some academic, political and social sectors have raised between public health and personal data protection in reductionist terms, putting forward a series of tautological arguments advocating the fervent defense of public health to the detriment of the fundamental rights of privacy, which, as we have pointed out, not only can't be suspended in any way by the declaration of the State of Alarm, but also constitute the foundation of a set of constitutionally recognized human rights that now a days with the increasing processes of digitalization and datafication of society acquires a huge importance.

In our opinion, it is not true that personal data protection and its powerful regulation led by the European GDPR are presented as obstacle elements which would make it difficult to implement and process the necessary personal data for the adoption of effective measures in relation to COVID-19; nothing further from the reality of what is being pursued, and we have made this clear in the preceding pages, the correct application of an advanced regulation geared to protect a fundamental right, such as personal data protection, includes among its articles the performance of actions of processing personal data in an atypical or unexpected scenarios such as the one we find ourselves in. Therefore, from our point of view – perhaps impregnated by the historical development and the marked humanist character of the Salamanca study that we follow – is that, 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 an emergency context such as the one we have had to live, it is impossible to achieve a certain guarantee of public health without safeguarding high standards of personal data protection, which, as we have already insisted, is the basic institute for the full effectiveness and guarantee of all constitutionally recognized fundamental rights, establishing itself as the cornerstone of the Social and Democratic State of Law in the digital (r)evolution era.

All of these arguments require from health authorities to be particularly careful when adopting measures that may have irreversible consequences on citizens fundamental rights only guided by urgency, fear or other suspicious interests. At this point, it should be remembered that information technologies cannot be understood in isolation, but always within the framework of a targeted treatment. This treatment should implement a comprehensive strategy based on scientific evidence, assessing its proportionality in relation to its effectiveness, efficiency and objectively taking into account the necessary organizational and material resources; without losing sight on the requirements of the new regulation on personal data protection, which has been conceived by the European Union with a strong humanistic inspiration. As the fourth whereas of the European General Data Protection Regulation states emphatically, «*the processing of personal data must be designed to serve humanity*».

5. REFERENCES

COTINO, Lorenzo. Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos. **IDP. Internet, Derecho y Política**, Barcelona, n. 31, pp. 1-17, 2020.

CRUZ, Marcio, SANTOS, Edgar, VELÁZQUEZ, Manuel, y LEÓN, Moisés. COVID-19, una emergencia de salud pública mundial. **Revista Clínica Española**, s.l., p. 1-7. 2020.

DOMÍNGUEZ, José Luis. **Comentario al Real Decreto-Ley 14/2019**, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Un paso más hacia la configuración de una regulación efectiva del ciberespacio. AIS: Ars Iuris Salmanticensis, Salamanca, vol. 8, n. 1, p. 217-223, 2020.

EUROPEAN DATA PROTECTION BOARD. **EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic**, Brussels, 14 April, 2020.

FERNÁNDEZ, Tomás Ramón. El Estado de Derecho, a prueba. In BLANQUER, David (Coord.). **COVID-19 y Derecho público (durante el estado de alarma y más allá**). 1st Edition. Valencia: Tirant lo Blanch, 2020, p. 19-24.

FERNÁNDEZ DE GATTA, Dionisio. Los problemas de las medidas jurídicas contra el coronavirus: las dudas constitucionales sobre el Estado de Alarma y los excesos normativos. **Diario La Ley,** Madrid, n. 9634, p. 1-21, 2020.

FERNÁNDEZ DE GATTA, Dionisio. **El estado de alarma por la epidemia del coronavirus y sus problemas constitucionales legales.** AIS: Ars Iuris Salmanticensis, Salamanca, vol. 8, n.1, p. 27-40, 2020.

FERRETTI, Luca, WYMANT, Chris, KENDALL, Michelle, ZHAO, Lele, NURTAY, Anel, ABELER, Lucie, PARKER, Michael, BONSALL, David, FRASER, Christophe. Quantifyng SARS-CoV-2 transmission

suggest epidemic control with digital contact tracing. **Science**, Washington-D.C, vol. 368, n. 6491, p. 1-29, 2020.

LOZANO, Blanca. Análisis de urgencia de las medidas administrativas del estado de alarma. **Diario La Ley**, Madrid, n. 9601, p. 1-11, 2020.

MARTÍNEZ, Ricard. Covid-19 ¿hacia un rediseño de la privacidad?. **La Ley Privacidad**, Madrid, n. 5, 2020.

MARTÍNEZ, Ricard. Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. **Diario La Ley**, Madrid, n. 9601, p.1-11, 2020.

MEDINA, Manuel. Categorías especiales de datos. In RALLO, Artemi (Dir.). **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**. 1st Edition. Valencia: Tirant lo Blanch, 2019, p. 251-274.

MOZUR, Paul, ZHONG, Raymond, KROLIK, Aaron. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. **New York Times**, New York, 2020.

NATIONAL CRYPTOLOGICAL CENTRE. **Inform BP/18.** Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia**,** Madrid, 2020.

NISHIURA, Hiroshi, KOBAYASHI, Tetsuro, MIYAMA, Takeshi, SUZUKI, Ayako, JUNG, Sung-mok, HAYASHI, Katsuma, KINOSHITA, Ryo, YANG, Yichi, BAOYIN, Yuan, AKHMETZHANOV, Andrei, LINTON, Natalie. Estimation of the asymptomatic ratio of novel coronavirus infections (COVID-19). **International journal of infectious diseases**, s/l, n. 94, p. 154-155, 2020.

PIÑAR, José Luis. El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. **Asamblea. Revista Parlamentaria de la Asamblea de Madrid**, Madrid, n. 13, p. 21-46, 2005.

PIÑAR, José Luis. Transparencia y protección de datos en el estado de alarma y en la sociedad digital post COVID-19. In BLANQUER, David (Coord.). **COVID-19 y Derecho público (durante el estado de alarma y más allá**). 1st Edition. Valencia: Tirant lo Blanch, 2020, p. 135-184.

PIÑAR, José Luis. Privacidad en estado de alarma y normal aplicación de la Ley. **Hay Derecho**, **Expansión**, Madrid, abril, 2020.

PIÑAR, José Luis. 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**, Madrid, n. 3, 2020.

PUENTE, Agustín. Principios y licitud del tratamiento. *In* RALLO, Artemi (Dir.). **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**. 1st Edition Valencia: Tirant lo Blanch, 2019, p. 115-168.

PUYOL, Javier. Los principios del derecho a la protección de datos. *In* PIÑAR, José Luis (Dir.). **Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad**. 1st Edition. Madrid: Editorial Reus, 2016.

QIU, Haiyan, WU, Junhua, HONG, Liang, LUO, Yunling, SONG, Qifa, CHEN, Dong. Clinical and epidemiological features of 36 children with coronavirus disease 2019 (COVID-19) in Zhejiang, China: an observational cohort study. **The Lancet Infectious Diseases,** London, vol. 20, p. 689-696, 2020.

SALAS, Sofía. Consideraciones éticas respecto del "pasaporte" COVID-19. **Revista chilena de infectología**, Santiago de Chile, vol. 37, n. 3, p. 329-330, 2020.

SPANISH DATA PROTECTION AGENCY. **Legal Report 0017/2020**, Madrid, 2020, p. 1-7.

SPANISH DATA PROTECTION AGENCY. **Comunicado en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos**, Madrid, 2020.

SPANISH DATA PROTECTION AGENCY. **Comunicado en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos**, Madrid, 2020.

SPANISH DATA PROTECTION AGENCY. **Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo,** Madrid, 2020, p. 1-6.

SPANISH DATA PROTECTION AGENCY. **El uso de las tecnologías en la lucha contra el COVID19,** Madrid, 2020, p. 1-13.

TERRÓN, Daniel, DOMÍNGUEZ, José Luis. **Nueva regulación de la protección de datos y su perspectiva digital**. 1st Edition. Granada: Comares, 2019.

TERRÓN, Daniel, DOMÍNGUEZ, José Luis, y FERNANDO, Marcos Matías. Los derechos fundamentales de la privacidad: derecho y necesidad en tiempos de crisis. **Revista General de Derecho Administrativo**, Madrid, n. 55, p. 1-31, 2020.

VOO, Teck Chuan, CLAPHAM, Hannah, TAM, Clarence. Ethical Implementation of Immunity Passports During the COVID-19 Pandemic. **The Journal of infectious diseases**, Oxford, vol. 222, n. 5, p. 715-718, 2020.