MASTER UNIVERSITARIO EN ASESORÍA JURÍDICA DE EMPRESAS

2020/2021

PROYECTO FIN DE MASTER

<El derecho a la protección de datos y COVID19. Especial significación en el ámbito laboral>

Autor: D. Pedro Rodríguez Jurado

Tutora: Dª Carmen García Ruíz

JUNIO 2021

INDICE

ABREVIATURAS

- Agencia Española de Protección de Datos: **AEPD**
- Comité Europeo de Protección de Datos: **CEPD**
- Constitución Española**: CE**
- Evaluación de impacto de protección de datos: **EIPD**
- Ley de Medidas Especiales en Materia de Salud Pública: **LMESMP**
- Ley Orgánica De Regulación Del Tratamiento Automatizado De Los Datos De Carácter Personal: **LORTAD**
- Ley Orgánica de Protección de Datos de Carácter Personal : **LOPD**
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales: **LOPDPGDD**
- Ley General de Salud Pública: **LGSP**
- Reglamento Europeo de Protección de Datos: **RGPD**
- Ley de prevención de Riesgos Laborales; **LPRL**
- Secretaria General de Administración Digital: **SGAD**
- Unión Europea: **UE**

RESUMEN

La COVID19 y sus consecuencias sociales, políticas y económicas han resultado devastadoras en todos los sentidos. Por desgracia, ha afectado en mayor medida a aquellos que no se encontraban preparados para este tipo de enfermedades, siendo en mayor medida las que menos recursos tenían antes del inicio de la pandemia. Los esfuerzos de los gobiernos se han centrado en aprovechar todos los medios disponibles para evitar la propagación del virus.

Uno de ellos ha sido la utilización de la tecnología para poner a disposición de las autoridades el acceso a nuestros datos. Precisamente va a ser nuestro tema de investigación, en conocer hasta qué punto una situación como la vivida permite o no el tratamiento de nuestros datos que en otras circunstancias no se podría haber llevado a cabo. Es decir, si evitar la propagación del virus es causa suficiente como para que pueda afectarse nuestra intimidad. Se realizará un juicio de valor entre ambas esferas (PRIVACIDAD VS COVID 19) en el que comprobaremos como una de ellas primará sobre la otra.

Haremos hincapié en los instrumentos utilizados por nuestro país para evitar la propagación del virus que han podido afectar a la protección de la privacidad y su puesta en práctica; y nos detendremos en la incidencia que este derecho tiene en el ámbito laboral, y muy especialmente, durante la pandemia del COVID-19

Palabras clave: COVID 19, protección de datos, intromisión, legalidad, salud pública, datos sensibles, relaciones laborales

ABSTRACT

COVID19 and its political, economic and social consequences have been devastating in every way. Unfortunately, it has most affected those who were unprepared for this type of disease, and those who had the least resources before the start of the pandemic. Government efforts have focused on using all available means to prevent the spread of the virus.

One of these has been the use of technology to give authorities access to our data. This is precisely the subject of our research, to find out to what extent a situation such as the one we have experienced does or does not permit the processing of our data, which in other circumstances could not have been carried out. In other words, whether preventing the spread of the virus is sufficient cause for our privacy to be affected. A value judgement will be made between both spheres (PRIVACY VS COVID 19) in which we will see how one of them will prevail over the other.

We will emphasize the instruments used by our country to prevent the spread of the virus that may have affected the protection of privacy and its implementation; and we will focus on the impact that this right has in the workplace, and very especially, during the COVID-19

Keywords: COVID 19, data protection, meddling, legality, public health, sensitive data, labor relations

INTRODUCCION

El derecho a la protección de datos es un tema candente en nuestros días. Aún más en los momentos en los que se realiza esta investigación, pues ha sido en esta pandemia provocada por la COVID-19 como este derecho ha ido cobrando más relevancia. Si bien nos encontramos ante un derecho que se encontraba normativizado desde el siglo pasado, ha estado en constante transformación, provocado en gran medida por lo íntimamente relacionado que se encuentra con los instrumentos con los que se pueden recopilar nuestros datos.

Prueba de ello es, que como veremos a lo largo de esta investigación, el punto de partida del derecho a la protección de datos se encuentra en el secreto de las comunicaciones postales, no pudiéndose hablar de "datos" en sentido estricto. El ámbito de aplicación y la esfera de protección que este derecho otorga no ha hecho sino extenderse a lo largo de los años.

Cabe decir que este derecho se ha ido adaptando de una forma muy satisfactoria a las nuevas realidades, apreciándose en elementos como los nuevos dispositivos susceptibles de guardar información; o en las distintas categorías por las que nuestros datos se encuentran agrupados.

La protección de estos derechos, aspecto que los diferencia respecto de otros, se realiza desde una doble perspectiva: el acceso y el tratamiento, más intensificado en el segundo. Por ello, a la hora de hablar del derecho a la protección de datos, sería más acertado preguntarnos no tanto el ¿qué?-se protege sino el ¿cómo?-se debe actuar ante estos datos.

Otro elemento diferenciador es que conviven dos sujetos en esta protección: la persona y sus datos. No obstante, y como veremos a lo largo de estas líneas, la respuesta decaerá sobre la protección del segundo sobre el cual, nosotros como portadores de esta información, tenemos un gran poder de decisión sobre ellos, por lo que como no podía ser de otra forma, se encuentran íntimamente relacionados.

Todas estas incógnitas se han puesto de manifiesto con la pandemia de la COVID-19, la cual ha supuesto numerosos retos principalmente en el ámbito de la salud, y también en el terreno de la protección de datos, los cuales, como se ha podido comprobar, han resultado de gran ayuda para evitar la propagación del virus. No obstante, tal y como la legislación se ha encargado, esta intromisión no debe de realizarse bajo cualquier pretexto, y es precisamente en lo que nos vamos a ocupar en esta investigación bajo los siguientes interrogantes:

Este contenido se realizará respondiendo a las siguientes preguntas que han ido surgiendo durante la investigación de este asunto, y son las siguientes, pudiéndolas definir como objetivos de la investigación:

- ¿Es el derecho a la protección de datos un derecho fundamental?
- ¿Qué aspecto está realmente protegido: su acceso o su tratamiento?
- ¿Se ha podido ver suspendido/restringido por el Estado de Alarma?, o si por el contrario, ¿su legislación prevé que por motivos sanitarios estos datos están a disposición de la finalidad publica?
- ¿Ha sido la pandemia una situación excepcional para la aplicación de las reglas de protección de datos?
- ¿Hasta dónde es admisible la intromisión en la privacidad del individuo para proteger la salud pública?
- En caso de existir limites ¿Se han transgredido durante la pandemia del COVID?

Por último, y para acercar lo máximo posible esta investigación con la realidad, analizaremos el impacto que ha tenido la protección de datos en el ámbito laboral durante la pandemia, haciendo especial referencia al uso de datos sanitarios.

De un modo esquematizado y estructurado estos serian los objetivos de investigación:

I. Analizar la normativa de protección de datos a distintos niveles y como se interrelacionan entre sí, además de conocer la naturaleza jurídica de este derecho.
II. Conocer el impacto que ha tenido la crisis del coronavirus en el derecho a la protección de datos.
III. Explorar si la normativa reguladora adapta el tratamiento de datos a la situación de pandemia; o si, por el contrario, ha sido necesario el Estado de Alarma para que su protección se encuentre restringida
IV. Conocer las bases jurídicas que permiten el tratamiento de nuestros datos y sus límites.
V. Comprobar en la práctica si durante esta pandemia se ha cumplido con los principios que rigen el tratamiento de nuestros datos.
VI. Analizar el acceso a nuestros datos por parte de los empleadores, y más en concreto, respecto de los datos relativos a nuestra salud.

Para responder al primer y tercer objetivo se realizará un análisis exhaustivo de los instrumentos jurídicos que regulan la normativa del derecho a la protección de datos desde sus inicios, concretando las novedades legislativas. Para ello se han utilizado las bases de datos que contienen estas normas como Vlex o el propio catálogo de la Biblioteca de la Universidad de Loyola.

En el caso del segundo objetivo, serán los artículos doctrinales relacionados con este tema de investigación los que nos aportarán luz al contenido. Se ha realizado la búsqueda en las bases de datos correspondientes, acudiendo nuevamente a Vlex, DialNet o Lefebvre.

El tercer objetivo será resultado de aplicar lo estudiado a la situación real, comparando la normativa con su puesta en práctica. Para ello, serán las disposiciones emanadas de los

organismos competentes y los informes de la Agencia Española de Protección de Datos los que nos den las claves.

Para responder al cuarto objetivo será necesario analizar bajo qué circunstancias nos encontramos para que se habilite o no el tratamiento de datos personales; y bajo qué garantías se encuentras supeditadas. Será resultado de la aplicación de los instrumentos jurídicos mencionados anteriormente

Por último, se hará mención especial al tratamiento de datos en el ámbito laboral y su incidencia en las relaciones laborales. Por una parte, se determinará la base jurídica contenida en la normativa, al mismo tiempo que lo concretaremos con la visión de artículos doctrinales.

Realizadas las consideraciones previas a la elaboración del Trabajo Fin de Master, damos comienzo a su contenido.

1. REGULACION DEL DERECHO A LA PROTECCION DE DATOS

1.1 PROTECCION DE DATOS A NIVEL INTERNACIONAL

Del secreto de las comunicaciones postales a la protección de datos de carácter personal

El alcance de la protección de datos como lo conocemos en la actualidad ha sufrido un largo y constante proceso de evolución, acompañado por una serie de factores que veremos posteriormente. Si en la actualidad podemos encontrar debates jurídicos en torno a una situación concreta sobre qué derechos priman sobre otros, las primeras manifestaciones del

derecho a la protección de datos parecían no encontrar cabida. Prueba de ello es que la protección de la propiedad literaria primaba sobre la protección a la intimidad. Lleva a considerar que la protección de datos personales no era concebida como un derecho que había que asegurar.

Una sentencia celebérrima fue la conocida *Jones vs Tapling* (1865) por la cual el Tribunal de la Cámara de los Lores desestimó las pretensiones de un demandante que se quejaba de que las ventanas de su vecino permitían la vista de sus propiedades, lo que suponía una vulneración de su intimidad. El fallo, aun ajeno a la protección de la intimidad como se encuentra reconocida hoy en día, llega a afirmar claramente que "privacy is not a right" y que sólo la intromisión física en la propia propiedad daba lugar a una protección jurídica

El hito que marca el reconocimiento de este derecho es la obra jurídica: "The right to privacy" (Warren & Brandeis, 1890) Aún lejano al concepto de privacidad que entendemos hoy en día, sigue siendo concebida como el derecho a ser dejado solo o a no ser molestado. Si bien no tuvo una gran trascendencia en el momento de su publicación, se considerará tiempo después el ensayo fundacional de la protección de la esfera privada estadounidense. (Saldaña, 2012)

La primera Ley en materia de protección de datos es la emanada del Land alemán de Hesse (1970), llegándose a considerar el instante de su aprobación como momento de nacimiento de este derecho (Cruz, 1989). Esta ley amplia el concepto de protección a la intimidad tal y como se venía entendiendo por las obras mencionadas anteriormente, a la protección de datos de una persona. Son las necesidades que tenía la administración pública para recoger los datos de sus ciudadanos lo que motivo que se aprobara esta ley. Por ello, tenía la finalidad de regular la privacidad de los datos personales de los ciudadanos con respecto a la administración pública de dicho Land.

Aunque podríamos considerarla como una Ley cercana a lo que entendemos como protección de datos en la actualidad, el título era en realidad un nombre inapropiado, ya que la Ley no protegía los datos, sino los derechos de las personas cuyos datos se estaban tratando (Burkert, 2000),. En cuanto a sus novedades, esta ley también introdujo la primera autoridad independiente de protección de datos. Una figura similar a lo que entenderíamos como el delegado de Protección de Datos hoy en día.

Mas allá de sus detractores, sienta las bases de lo que entendemos hoy como derecho a la protección de datos. Como regla general se consideran los datos personales sometidos a tratamiento por el Land como confidenciales, lo que supone que el concreto tratamiento de la cesión o comunicación de datos está necesitada una legitimación especial, que en el caso de esta ley todavía están lejos de la voluntad del interesado: son las previsiones legales, o bien una orden expresa de quienes tienen encomendada la supervisión o control de los procesos informáticos del Land.

Se reconocen los derechos de rectificación y de oposición , y se establece un órgano de supervisión independiente.

Con la aprobación de esta ley se trataba de evitar que se convirtiera en realidad la visión orwelliana del estado omnipotente, que éste pudiera acceder a los aspectos más íntimos de la vida humana y que pudiera manipular a las personas a través de los datos personales. (Pascual, 2017)

Acercándonos un poco más a la legislación actual, nos encontramos con las leyes suecas de 1973, convirtiéndose en el primer Estado del mundo en regular a nivel nacional (el Land se refería a un concreto territorio, era de alcance regional) el uso de los datos personales a través de sistemas informatizados. Aunque pudiera pensarse que la primigenia es la de Hessen vista anteriormente, ésta es considerada como tal debido a su intención de abarcar un mayor campo de actuación, incluyéndose desde este momento al ámbito privado.

En otro sentido, y en muestra de la modernización legislativa que supuso esta “Ley de datos” se encuentra la categoría de los conceptos utilizados.

Mientras que en la Ley de Hesse aparecían por primera vez en un texto normativo los conceptos de datos, banco de datos, protección o tratamiento de datos; la Ley Sueca va más allá y comienza a emplear términos como “información o datos de carácter personal, o incluso el concepto de datos sensibles, el cual ostentaba un tratamiento más restringido. En relación con nuestra línea de investigación, se encontraban los relativos a los datos de salud. (Pascual, 2017)

Estas leyes mencionadas han contribuido enormemente a la base legislativa de la mayoría de los estados, los cuales, además de la propia Alemania y Suecia, países como Francia, Dinamarca y Noruega han ido modernizando estos textos hasta convertirlos en lo que los conocemos hoy en día

El primer instrumento a nivel internacional, jurídicamente vinculante, en el ámbito de la protección de datos de carácter personal es el Convenio N.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. En la actualidad, vincula a un total de 51 Estados, incluyéndose otros que no pertenecen la Unión Europea. Supone un avance en cuanto a los conceptos utilizados, otorgando mayor seguridad jurídica: "datos personales", "controlador", "instrumento" y “tratamiento”. Recoge por primera vez una serie de principios que han sido los que se han ido aplicando posteriormente, sin perjuicio de otros que se han ido añadiendo. Merecen mención pues a lo largo del trabajo recurriremos a ello en más de una ocasión: Principio de Limitación de Recogida, Principio de Calidad de Datos, Principio de Especificación de Propósitos y Principio de Limitación de Uso . (Artículo 5); . Principio de seguridad de los datos (Articulo 7); y Principios de apertura y participación individual (Articulo 8).

El Convenio añadió a estos un artículo especial sobre el tratamiento de "categorías especiales de datos", es decir, "datos personales que revelan origen racial, opiniones políticas o creencias religiosas o de otro tipo, así como datos personales relativos a la salud o la vida sexual" y "datos personales relacionados con condenas penales" (Articulo 6).

Se estipuló que dichos datos, comúnmente denominados "datos confidenciales", "no se tratarán automáticamente a menos que la legislación nacional establezca garantías adecuadas". (Douwe & Maria, 2019)

Estos datos confidenciales son los que mas han tenido impacto en la pandemia, y ya desde este Convenio se contenían las salvaguardas acerca de su tratamiento, que son precisamente, a los que acudiremos posteriormente para medir las actuaciones de los distintos responsables del tratamiento de estos datos.

En este primer epígrafe se ha dado cuenta del desarrollo que ha sufrido esta categoría de derechos, considerado desde el principio como fundamental. Prueba de ello es que en un principio ha sido negada su existencia, encontrando sus orígenes en el derecho a la privacidad, igualmente rechazada (Jones vs Tapling); y nos encontramos ante un escenario en el que, no solo se reconoce y se otorga seguridad jurídica a estos derechos, sino que se es consciente de la entidad de los distintos datos que nos pueden identificar, y que, por tanto, merecen especial consideración.

1.2 PROTECCION DE DATOS A NIVEL EUROPEO

El Convenio no había dado lugar a una protección amplia o armonizada, en general, de los datos personales en la Comunidad: para septiembre de 1990, solo había sido ratificada por siete Estados miembros de la CE (aún no había adoptado la legislación pertinente), y las leyes

en esos Estados miembros diferían considerablemente en aspectos importantes. (Douwe & Maria, 2019)

Fruto de esta necesidad de armonización, nace la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Con la libre circulación de mercancías, resultaba necesario habilitar la libre circulación de datos de carácter personal de un Estado miembro u otro. Este flujo de datos hacia imprescindible una armonización de las legislaciones nacionales con el fin de evitar cualquier obstáculo al flujo transfronterizo.

No obstante, de la propia naturaleza del instrumento elegido se puede sospechar que el problema de armonización no iba a ser resuelto. Sus disposiciones debían ser transpuestas a la legislación nacional por los Estados miembros, y para esto, a los Estados miembros se les otorgó discreción considerable, lo que condujo a considerables divergencias entre las legislaciones nacionales de los Estados miembros que aplicaban.

.

Una importante nueva característica de la Directiva de 1995 fue que, para conseguir una mayor armonización entre las leyes de los Estados miembros, establecía en el artículo 7 una lista exhaustiva de "criterios para legitimar el tratamiento de datos", lo que más tarde se denominaría "bases jurídicas" para el tratamiento de datos personales, (Douwe & Maria, 2019) que son las que nos darán las claves en muchos aspectos de nuestro trabajo.

La normativa europea evoluciona hasta aprobar el Reglamento 2016/679 de 27 de abril de 2016 relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, completado con la Directiva 2016/680 de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecto al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención,

investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

Esta norma trata de superar las dificultades propias de una Directiva, naciendo con el objetivo de unificar y modernizar la normativa europea sobre protección de datos, permitiendo a los ciudadanos un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores.

Entre sus principales novedades se encuentra en la ampliación de los derechos que se le otorgan a los ciudadanos respecto de sus datos personales, dejando atrás los conocidos como derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en España, para dar paso a derechos de Transparencia (art. 12), Información (arts. 13 a 14), Acceso (art. 15), Rectificación (Art. 16), Supresión o derecho al olvido (art. 17), Limitación del tratamiento (art. 18), Portabilidad de datos (art. 20) y Oposición (art. 21).

1.3 PROTECCION DE DATOS A NIVEL NACIONAL

El primer reconocimiento que se hace sobre el derecho a la protección de datos en nuestro país es en la constitución de 1978. Del encaje constitucional podemos deducir que desde un principio se le concebía como un derecho fundamental, pues su articulo 18.4 se encuentra dentro de la sección que la carta magna otorga tal consideración.

En puridad, no nos encontramos ante la protección de los datos personales de los ciudadanos, pues atendiendo a su literalidad,

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

el derecho a la protección de datos no se configura en este primer momento como un derecho independiente, sino vinculado al derecho a la intimidad, al honor personal y familiar y al pleno ejercicio de sus derechos. (Fernandez J. M., 2003)

Será la Sentencia del Tribunal Constitucional 11/1998, de 13 de enero, la que primero introduzca el término «privacidad» en el ámbito de la protección de datos y como un concepto distinto al de intimidad, siendo el primero un término que abarca un ámbito más amplio que el de la intimidad. (Lorenzo & Reyes, 2002)

La primera ley la encontramos en la Ley Orgánica De Regulación Del Tratamiento Automatizado De Los Datos De Carácter Personal (LORTAD), que fue la que introdujo los derechos ARCO. Data de 1982, y en consonancia con lo visto anteriormente, fue modernizada por los sucesivos instrumentos normativos europeos.

No obstante, nuestro país acusó la falta de transposición de la Directiva que mencionamos anteriormente, y la llevó a cabo excediéndose del plazo concedido. No fue hasta 1999 cuando la transposición de esta directiva dio lugar a la aprobación en nuestro país de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), que supuso la derogación de la LORTAD

La transposición tardía por parte de España provocó además que la LOPD conviviera hasta 2008 con disposiciones reglamentarias que desarrollaban la ya desfasada LORTAD. No fue sino hasta la entrada en vigor del RD 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD.

Serán la LORTAD y la LOPD las que, conforme al artículo 18.4 del RGPD desarrollaran el contenido de este derecho, el cual se ha visto actualizado conforme a las necesidades que se iban sucediendo y a la adaptación a nivel nacional de los textos normativos europeos que se iban aprobando como vimos anteriormente.

Para no extendernos demasiado en su génesis, y a modo de acercar lo máximo posible esta investigación a la actualidad, haremos más hincapié en la Ley de Protección de Datos Personales y garantía de los Derechos Digitales (LOPDPGDD), la sucesora de la LOPD.

La primera novedad deriva de la segunda parte de su título, pues hace referencia a una nueva categoría de derechos, los digitales. Nos encontramos ante un nuevo escenario, en el que la ley recoge los derechos digitales y libertades del entorno de Internet tales como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital ,así como los derechos al olvido, a la portabilidad y al testamento digital, junto con el derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet; más la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Otra novedad que merece mención es que el ámbito de aplicación se amplía a los fallecidos. Se abre la posibilidad para sus familiares, herederos o quienes designe el fallecido, de ejercer los derechos de acceso, rectificación y supresión en su nombre. Es prueba de que estamos ante un conjunto de derechos de constante evolución, es que se establezca que el consentimiento para el tratamiento de datos personales sea válido para las personas mayores de 14 años. Se es consciente de que el acceso a internet está más presente en edades más cortas.

El consentimiento es una figura muy importante dentro del articulado de esta ley. Ya desde el RGPD se le reconoce como uno de los supuestos para el tratamiento de nuestros datos. Por tanto, el acceso a nuestros datos no es indiscriminado, sino que previamente hemos de declarar expresamente que consentimos el tratamiento de estos. Deberá ser prestado de forma libre, específica, informada, inequívoca, y en una declaración o una clara acción afirmativa.

Se añade además una nueva categoría de datos, ampliando los supuestos de permisividad en el tratamiento de este tipo de datos cuando estén amparados en una norma con rango de ley,

que podrá cubrir el tratamiento de datos de salud cuando sea exigido por la gestión de los sistemas, servicios de asistencia sanitaria y social o la ejecución de un contrato de seguro.

Hacemos referencia a las bases jurídicas que fueron desarrolladas en la Directiva 96/46 que, pese a sus dificultades en su aplicación ha sentado las bases de los sucesivos instrumentos normativos. Se encuentran en el artículo 9 de la RGPD al que vamos a acudir en numerosas ocasiones para determinar qué circunstancia ha posibilitado el tratamiento de nuestros datos. Dependiendo de la categoría de estos, será válido el consentimiento, la ejecución de un contrato, o motivos de salud pública.

2. PROTECCION DE DATOS Y COVID 19

Analizaremos de qué manera se ha podido ver afectado el derecho a la protección de datos durante la pandemia del coronavirus que hoy seguimos padeciendo.

De lo visto en estas líneas, podemos llegar , de forma muy sintética a la siguiente conclusión: estamos ante un derecho fundamental que, bajo una serie de premisas, se puede ver restringido.

Ya con carácter general la presidencia del Comité Europeo de Protección de Datos hizo pública el pasado 16 de marzo una declaración sobre el tratamiento de datos personales en el contexto de la crisis del Covid-19, en la que resalta que la normativa sobre protección de datos y en particular el Reglamento 2016/679, no impiden tomar medidas en la lucha contra la pandemia del coronavirus, pero advierte que incluso en estas excepcionales circunstancias quienes traten datos personales deben asegurar su protección. Sin perjuicio de que el propio RGPD y la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas prevén reglas que pueden aplicarse al tratamiento de datos que se lleve a cabo en un contexto como el

actual, que permitiría incluso obviar en ciertos casos el consentimiento de los afectados. (Piñar, 2020)

No obstante, resulta obvio que todo derecho fundamental ante situaciones excepcionales se puede ver suspendido. Lo particular en este sentido en cuanto al derecho a la protección de datos, es que no es necesario que exista una disposición que expresamente limite su aplicación, puesto que ya la ley lo prevé.

Yendo más allá, el derecho a la protección de datos no se ha visto suspendido en ningún momento por la crisis del COVID-19. Si analizamos el Real Decreto 463/2020 de 14 de marzo y el Real Decreto-Ley de 17 de marzo de 2020 por el que se establecían medidas excepcionales, vemos como el único derecho fundamental limitado es el de la circulación. Por ello, para ser más correctos, no conviene hablar de "restricción" o "suspensión" de derechos en el caso de la protección de datos, aun estando en situación de pandemia. Como veremos posteriormente, la ley permite bajo ciertas circunstancias, entendidas como base jurídica, el tratamiento de nuestros datos. (Timón, 2020)

Conviene insistir en que la declaración del estado de alarma no permite limitar derechos y libertades más allá de lo que dispone el artículo 11 de la Ley Orgánica 4/1981 de los estados de alarma, excepción y sitio. Es más, en ningún caso pueden suspenderse derechos, sino tan sólo adoptar medidas que, con la imitación señalada, condicionen su ejercicio. Así debe interpretarse el artículo 55.1 de la Constitución que tan sólo permite suspender derechos cuando se declare el estado de excepción o de sitio, pero no el de alarma. Y aun así no todos los derechos pueden ser suspendidos, sino sólo los reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2 de la Constitución. (Piñar, 2020)

El derecho a la protección de datos deriva del artículo 18.4 de la Constitución, como declaró ya hace tiempo el Tribunal Constitucional en su Sentencia 292/2000 de modo que ni

siquiera en los estados de excepción y sitio puede ser suspendido; mucho menos, pues, en el estado de alarma (Piñar, 2020)

De esta cuestión ya se ocupó el INFORME 0017/2020 emitido por el gabinete jurídico de la AEPD (Agencia Española de Protección de Datos) para concluir lo siguiente: *"la normativa de protección de datos personales, en tanto que, dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada"*

Esto no significa que la protección de datos se haya sido ajena a la pandemia, en el sentido de que esta crisis no haya tenido efectos sobre su contenido y aplicación. Resulta comprensible que la protección de datos no deba utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades en la lucha contra la pandemia, tanto desde un punto de vista práctico, pues la misión principal es la de salvar vidas; como que esta premisa ya se encuentra recogida en la normativa de protección de datos, cuya regulación compatibiliza y pondera los intereses y derechos en liza por el bien común. (INFORME 0017/2020)

La protección de datos y la lucha contra la pandemia deben ejercerse de forma complementaria, no debiendo dejar vacío de contenido al primero, llegando a una de las primeras claves de nuestro trabajo de investigación: el equilibrio, que como hemos visto, se encuentra perfectamente normativizado.

Ya desde el RGPD se reconoce que no estamos ante un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad (considerando 4), llegando a otro concepto clave que nos acompañará en nuestro trabajo. Lo podríamos considerar como la traducción jurídica de equilibrio, si bien considero que mientras este se refiere a las situaciones concretas en las que se puede ver restringido el derecho a la protección de datos; la segunda se encuentra más dirigida al modo en el que este derecho se restringe, para

evitar como hemos dicho, que ante una situación como la que vivimos actualmente, se pueda dejar vacío de contenido.

Esta teoría se manifiesta perfectamente a lo largo del articulado del RGPD, poniendo como ejemplo, los datos personales relativos a la salud.

A la vista del artículo 9.1[1], podríamos llegar a la conclusión de que el tratamiento de estos datos resulta totalmente prohibido, aunque inmediatamente en el apartado siguiente recoge una serie de excepciones que avalarían su tratamiento (Art. 9.2 RGPD). Está tratando de establecer un equilibrio entre la eficacia de un derecho fundamental con circunstancias que, dada su entidad, resulta necesario para proteger un interés esencial (considerando 46)

Es el mismo considerando 46 el que asimila el control de pandemias como situación merecedora de proteger un interés esencial, y es el mismo artículo 9.2.i) el que concreta legislativamente esta situación

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, (art. 9.2.i RGPD)

Pues bien, la legislación española, atendiendo al requerimiento del articulo 9.2.i) del RGPD para que sean los EEMM los que establezcan las medidas adecuadas, establece en la LOPDGDD que el tratamiento de estos datos fundados en el Derecho español deberá estar amparado en una norma con rango de ley, que podrá establecer requisitos adicionales relativos

[1] Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o las orientaciones sexuales de una persona física. (Art. 9.1 RGPD)

a su seguridad y confidencialidad. (art 9.2 RGPD) Podríamos considerarlas como garantías para no dejar inoperativo este derecho fundamental, respetando así el equilibrio entre ambas esferas antes mencionadas.

Así, el legislador español se ha dotado de las medidas legales necesarias oportunas para enfrentarse a situaciones de riesgo sanitario, como la Ley Orgánica 3/1986, 20 de 14 de abril, de Medidas Especiales en Materia de Salud Pública (LOMEMSP) (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) o la Ley 33/2011, de 4 de octubre, General de Salud Pública. (LGSP)

El artículo 3 de la LOMEMSP señala que: con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible. Del mismo modo, los artículos 5 y 84 de la LGSP contiene la posibilidad de adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades.

Ahora bien, los tratamientos de datos personales en estas situaciones de emergencia sanitaria, como se ha mencionado al principio de este informe, siguen siendo tratados de conformidad con la normativa de protección de datos personales (RGPD y LOPDGDD), por lo que se aplican todos sus principios, contenidos en el artículo 5 RGPD, y entre ellos el de tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad (en este caso, salvaguardar los intereses vitales/esenciales de las personas físicas), principio de exactitud, y por supuesto, y hay que hacer especial hincapié en ello, el principio de minimización de datos.

Sobre este último aspecto hay que hacer referencia expresa a que los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, sin que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos sigue aplicándose con normalidad, sin perjuicio de que, como se ha dicho, la propia normativa de protección de datos personales establece que en situaciones de emergencia, para la protección de intereses esenciales de salud pública y/o vitales de las personas físicas, podrán tratarse los datos de salud necesarios para evitar la propagación de la enfermedad que ha causado la emergencia sanitaria. (INFORME 0017/2020)

Respecto del principio de limitación de la finalidad en relación con supuestos de tratamientos de datos de salud por razones de interés público el RGPD es claro, cuando establece que:

El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. […] **Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.** (Considerando 54)

Precisamente es en lo que nos vamos a ocupar en este apartado, en el análisis de las medidas que han tomado las autoridades de nuestro país para frenar el avance de la pandemia que puedan haber afectado al ámbito de la protección de datos. Posteriormente, nos detendremos en profundidad en las medidas adoptadas en el ámbito de la empresa y su significación.

2.1 APLICACIÓN DATACOVID19

Este debate tiene su manifestación en España con la aprobación por el Ministerio de Sanidad de la Orden SND/29/2020, de 27 de marzo , en la que figuran una serie de encomiendas de gestión a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) para el desarrollo, entre otros, de la app DataCOVID19 para monitorizar a la población con el fin de contener la pandemia.

La conformidad con el marco legal de las medidas de seguimiento digital dependerá de si son medidas temporales, necesarias y adecuadas en función de un propósito claramente previsto y delimitado (la gestión de la situación de crisis sanitaria ocasionada por la COVID-19). (Márquez & Ortega, 2020)

Los objetivos de esta Orden con la creación de estas aplicaciones informáticas lo dejan bien claro: realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el COVID-19, ofrecer información al usuario sobre el COVID-19 y proporcionar al usuario consejos prácticos y recomendaciones de acciones a seguir según la evaluación. (Resolución Primera Orden SND/297/2020)

A continuación, recoge una de las cuestiones que más controversias suscita. La aplicación permitirá la geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar, y se permitirá su gestión a través de terceros.

Es necesario recordar que, para que pueda hablarse de afectación a la privacidad, debemos encontrarnos necesariamente ante información que identifique o haga identificable a una persona física (art.4 RGPD)

Bajo esta premisa, la geolocalización de las personas no necesariamente afecta a la privacidad o a la capacidad de disposición de nuestros datos personales, debiendo distinguirse, por un lado, la geolocalización anonimizada de aquella geolocalización que permite la

identificación del usuario de ese dispositivo de forma directa o indirecta. (Timón Herrero, 2020).

(i) En efecto, una geolocalización anonimizada, que parte de la aportación de datos por parte de los operadores de comunicaciones electrónicas de forma agregada y anónima, tal como se prevé en la disposición segunda de la Orden de la Secretaría de Tecnología , no plantea problemas de privacidad ni activa las garantías de la normativa de protección de datos si, realmente, se cumple con ese principio de anonimato. No se identifica aquí a ningún usuario, ni ello permite elaborar perfiles personales. No se cumple por tanto el presupuesto de susceptibilidad de identificación a que aludía anteriormente. En este tipo de geolocalización los datos son objeto de tratamiento de agregación precisamente para romper la cadena de identificación y hacer imposible la asociación de los datos a una persona física.

(ii) Supuestos distintos son los de la geolocalización de dispositivos móviles no anonimizada o que permiten identificar al usuario de forma indirecta. El acceso a dichos datos se puede fundamentar, entonces, bien en el consentimiento del propio usuario -que adopta una posición activa al descargase una determinada aplicación y permitir el acceso a su ubicación-, bien en la concurrencia de uno de los supuestos de tratamiento lícito previstos en la normativa de protección de datos, como pueda ser la garantía de la salud pública y el freno de la pandemia.

Para analizar si cumple con la normativa de protección de datos lo analizaremos desde dos puntos de vista: teoría y práctica.

Sobre el papel, es decir, atendiendo a la Orden Ministerial citada anteriormente el funcionamiento es el siguiente: está basado en el uso de la conexión Bluetooth que deben tener activados los dispositivos móviles. Cuando dos personas que la tienen descargada pasan más de 15 minutos juntos a menos de 1,5 metros de distancia, los dos dispositivos intercambian unas claves, elaborando así un registro anonimizado al que el propio usuario tampoco puede acceder ni descifrar. En caso de que uno de los dos haya dado positivo, se le notificará al otro

usuario tal condición, sin que su identidad quede revelada, lo que permitirá que esta persona pase a confinamiento domiciliario durante el tiempo previsto por las autoridades sanitarias, mitigando el riesgo de que, en caso de haber sido contagiado, pueda afectar a otras personas.

Se puede afirmar, que, en principio, las medidas decretadas en la Orden SND/297/2020 son ajustadas a Derecho, ya que a través de ellas las autoridades españolas sólo podrán procesar "anónimamente" los datos de ubicación proporcionados libremente por los ciudadanos, es decir, procesar los datos agregados de manera tal que las personas no puedan volver a identificarse, y exclusivamente para la gestión de la crisis del coronavirus. Coinciden con Rivas (2020) en que dichas medidas "no tienen por qué representar una intromisión ilegítima en la vida privada de las personas, la vulneración a los derechos de protección de su propia imagen, protección de datos, intimidad y libre circulación" (Márquez Carrasco, Ortega Ramírez, 2020)

En la misma línea se pronuncian otros autores (Timón, 2020) añadiendo que el verdadero reto se encuentra, entonces, en realizar una aplicación escrupulosa de tales principios y exigencias, controlando y sancionando los eventuales excesos.

Esta autora nos adelanta uno de los aspectos que más dificultades plantea el derecho a la protección de los datos durante la pandemia del COVID: su puesta en práctica, siendo precisamente nuestro siguiente aspecto para tratar. https://elderecho.com/proteccion-de-datos-de-caracter-personal-y-crisis-sanitaria-covid-19

En este sentido se ha podido comprobar que su funcionamiento no ha sido el esperado. Empecemos por el principio: un detalle esclarecedor, es que la AEPD no participó en el desarrollo de su aplicación, imposibilitando su labor de supervisión. Esto provocó que se lanzara un comunicado[2] lamentando su desconocimiento el día 23 de junio de 2020, casi 2

[2] Comunicado disponible en (página web) https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-participacion-de-la-aepd-en-la-app-de Ultima consulta: 16 de junio de 2021

meses después de la entrada en vigor de la Orden Ministerial vista anteriormente. Esto supuso además la apertura de un procedimiento con el fin de proteger los derechos y libertades de los ciudadanos, con el objeto de obtener información sobre las características de la app inmediatamente después del anuncio público del proyecto, dando lugar al requerimiento de solicitudes formales de información a la SEDIA puesto que ha impedido a la AEPD valorar su adecuación a la normativa de protección de datos personales con antelación.

Este comunicado de la AEPD desmentía al anuncio por el cual el Gobierno presentaba esta aplicación, en la que aseguraba que: "La Agencia Española de Protección de Datos ha participado en el proceso previo a la puesta en marcha de este piloto y participará también en la evaluación de los resultados para poder proponer mejoras que garanticen en todo momento la privacidad a los usuarios."[3]

Esta circunstancia ha provocado la denuncia (ANEXO I) ante la propia AEPD contra la Secretaría General de Administración Digital (SGAD), organismo encargado de la implantación de la App Radar COVID en España, para que investigue si la aplicación cumple con el RGPD y las directrices del Comité Europeo de Protección de Datos (CEPD).

En su denuncia, a la que se ha logrado tener acceso directo, solicita a la AEPD que confirme que esta aplicación cumple con los principios de licitud, lealtad, transparencia y responsabilidad proactiva (Art.5 RGPD), ya que la SGAD no ha publicado la Evaluación de Impacto sobre la Protección de Datos (EIPD) ni el código fuente, en contra de lo indicado expresamente por el CEPD. También denuncia que en la Política de Privacidad no se han definido las funciones y responsabilidades de las autoridades sanitarias de las CC.AA. que han

[3] Nota de Prensa disponible en: https://www.mineco.gob.es/stfls/mineco/prensa/noticias/2020/200623_np_gomera.pdf (MINISTERIO DE ASUNTOS TECNOLOGICOS Y TRANSFORMACION DIGITAL, 2020) Ultima consulta: 16 de junio de 2021

completado los procesos técnicos necesarios para integrar la aplicación en sus sistemas sanitarios (Art. 13 y 14 RGPD).

Entre otras de sus reclamaciones se encuentra que la SGAD no ha especificado de forma suficientemente clara las distintas finalidades del tratamiento y sus respectivas bases legitimadoras. (Art. 13 y 14 RGPD). Considero que esta es la carencia que más relevancia podría tener a efectos jurídicos, pues es el aspecto clave que habilita el acceso a nuestros datos.

Por último, SGAD tampoco ha especificado los plazos de conservación de los datos para fines de investigación científica o histórica o fines estadísticos en la Política de privacidad (Art. 9.2j y 89.1 RGPD).

Estas deficiencias son comparadas en la reclamación con los países de nuestro entorno, quedando España en una posición comprometida, pues en Italia o Alemania no se aprecian.

El 5 de octubre de 2020, la AEPD notificó la admisión a trámite de la citada reclamación, al entender que *"A tenor de la información preliminar de la que se dispone, se aprecian indicios racionales de una posible vulneración de la normativa en materia de protección de datos, sin perjuicio de lo que se determine en el curso de la tramitación." (ANEXO II)*

Esta denuncia, fue ampliada el 24 enero de 2021 para, por una parte, incluir a la totalidad de las CCAA ya que en virtud de acuerdo con la SGAD las primeras asumieron la gestión de los resultados de la aplicación.[4] y por otra, actualizar supuestas vulneraciones de la normativa en materia de protección de datos que no habían sido corregidos correctamente desde la primera denuncia

En el contexto descrito la publicación del código fuente de RadarCOVID fue tardía e incompleta, hecho incompatible nuevamente con los principios de transparencia y responsabilidad proactiva del artículo 5 del RGPD, en atención a la interpretación efectuada

[4] Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad, acerca de la aplicación "Radar COVID"

por el EDPB en sus Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19 3 publicadas el pasado 21 de abril de 2020, y que debían ser objeto de conocimiento de la SGAD

Se han introducido importantes cambios en la redacción de la Política de Privacidad, entre los que destaca una relevante rectificación. Ahora se reconoce que RadarCOVID sí trata datos personales (seudonimizados, pero no anónimos) y, por tanto, sus usuarios pueden reclamar sus derechos de protección de datos (acceso, rectificación, supresión, limitación y oposición), tal y como ha venido defendiendo el Comité Europeo de Protección de Datos. Sin embargo, en la propia aplicación, se ofrece a los usuarios una información errónea al indicar que RadarCOVID no trata ningún tipo de dato personal

La ampliación de la denuncia recuerda que sigue sin publicarse la evaluación de impacto, análisis que debía haberse efectuado antes de su lanzamiento, tal y como recomendaba encarecidamente el EDPB, al considerar que el tratamiento de datos en las aplicaciones de rastreo puede entrañar un alto riesgo. Y es que dicha evaluación resulta esencial, pues en función de su resultado, se debía consultar a la Agencia Española de Protección de Datos antes de poner en marcha la aplicación, tal y como hicieron Italia y Alemania que contaron con la aprobación previa y pública de sus respectivas autoridades nacionales.

También denuncia la brecha de seguridad ocurrida en la aplicación por la que numerosos periódicos se hacían eco. Este riesgo a la privacidad se manifestaba desde el principio, pues cuando un usuario de Radar Covid recibe la confirmación de su positivo, las autoridades de su comunidad autónoma deben darle un código. Si decide introducirlo en la app, su móvil mandará a un servidor implica que el usuario es positivo. Esas claves son las que permitirán al resto de usuarios comprobar si han estado cerca del nuevo positivo. Así, solo hay un momento en que los usuarios suben claves al servidor de Radar Covid: cuando son positivos. Aunque ese

tráfico esté cifrado y el contenido de la comunicación sea anónimo, si hay subida al servi. Quien tenga acceso al tráfico, por tanto, sabe quién lo es. (Pérez, 2020)

En otras palabras, la brecha de seguridad tenía que ver con el tráfico de datos y como solo los positivos eran los que enviaban datos al servidor, quien tuviera acceso a la información de tráfico podría ver quién estaba mandando esos positivos. (Fernandez S. , 2020)

La opción de acceso a esa información no está al alcance de cualquier usuario, pero su explotación va más allá de las operadoras telefónicas y de Internet. La empresa Amazon también tiene acceso a esa información: la subida al servidor se hace con un software de la compañía estadounidense, con lo que también puede comprobar qué móviles mandaban positivos. Además de grandes empresas, también tendría acceso cualquier individuo o empresa con la opción de entrar a la misma red wifi desde la que se envían las claves. (Pérez, 2020)

El Gobierno de España se vio obligado a introducir parches en los distintos servidores para asegurar la anonimización de las personas positivas de la siguiente forma: se enviarían falsos positivos al servidor mediante la app para que resultase imposible descubrir su identidad en caso de ataque.

Sorprende por una parte que esta técnica fuese implementada el 20 de octubre, tiempo considerable desde su lanzamiento; cuando, además, este mecanismo ya lo preveían los países de nuestro entorno. Todas estas circunstancias hacen presumir que la no publicación de la EIPD se encuentra íntimamente relacionada, pues el Gobierno ha ido poniendo “parches” a cada problema que iba apareciendo.

El pasado 8 de junio, la AEPD acordó el inicio de sendos Procedimientos Sancionadores contra: 1) Ministerio de Asuntos Económicos y Transformación Digital y 2) Dirección General

de Salud Púbica; a raíz de dicha reclamación por presunta vulneración del Reglamento General de Protección de Datos (RGPD)[5]

Respecto de las apps de geolocalización con datos pseudonimizados se limita a, en un informe explicar de forma general las ventajas y los riesgos que pueden tener estas aplicaciones, sin detenerse en ninguna en concreto. No obstante, ya advertía de que la anonimización no se encontraba 100% garantizaba en todos los casos, y que su éxito dependía de cuestiones ajenas a la tecnología. Una de ellas precisamente era que se alcanzase un número determinado de personas usuarias dada la voluntariedad tanto en su instalación como en su uso, en el sentido de ir actualizando los datos relativos a contagios para que otros usuarios fuesen advertidos.

Pues bien, a fecha de junio de 2021, los datos recogidos son los siguientes

- Descargas: 6,8 millones de personas, esto supone menos de un 15% de la población
- Casos positivos detectados: 42.000, lo que supone menos del 2% de los diagnósticos de los producidos desde el inicio de la pandemia.

Estas carencias en lo relativo a la protección de datos por los responsables en nuestro país pueden deberse a una serie de factores desde el punto de vista de la experiencia (Martinez, 2021):

1. Las autoridades de control son reactivas. Esto es, responden a consultas específicas, o conflictos concretos. En raras ocasiones abordan cuestiones generales salvo en guidelines.

2. Cuando se definen criterios en sus guías —-elaboradas ya sea mediante recursos propios, ya mediante el recurso a la subcontratación de expertos--, no existe una consulta o debate público en la conformación de sus criterios. Esto afecta seriamente tanto a la calidad del

[5] Noticia disponible en: https://www.vozpopuli.com/economia_y_finanzas/proteccion-de-datos-radar-covid.html Ultima visita: 17 de junio de 2021

resultado como la viabilidad de la implementación de recomendaciones muchas veces alejadas de la realidad material.

3. El enfoque del regulador casi siempre opera desde el derecho fundamental a la protección de datos a la realidad, y casi nunca a la inversa. Y ello, no significa tan solo que se pierdan de vista elementos cruciales en los tratamientos de datos personales, sino también que se obvie en más de una ocasión la necesaria ponderación de derechos

3. PROTECCION DE DATOS EN EL AMBITO LABORAL

Nos situamos ante otro escenario en el que el derecho a la protección de datos se ha podido ver alterado por la pandemia. La relación ya no se establece entre Gobierno-ciudadano, sino entre empresario y trabajador, dando cuenta de la distinta naturaleza jurídica que ostentan ambas relaciones en base únicamente a su denominación.

Comenzaremos por las posibilidades que tiene una empresa de acceder a los datos generales sus trabajadores que nos ayudarán a sentar las bases para averiguar si esta posibilidad en qué manera se ha visto afectada por la COVID-19, haciendo especialmente referencia a los datos relacionados con la salud.

En primer lugar, y respecto de aquellos datos que no estarían catalogados como sensibles, y, por tanto, no incluidos dentro del artículo 9 del RGPD, en base a las condiciones del artículo 6.1.b) del mismo, el tratamiento de datos sería perfectamente lícito e cuando sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. No solo resultaría aplicable esta letra para validar el acceso a nuestros datos por parte de la empresa, ya que encontramos otras situaciones recogidas en este artículo que van encaminadas a hacerlos accesibles cuando sea necesario para cumplir con una obligación legal (art.61.b), como por ejemplo las de la Seguridad Social o las tributarias.

Como se puede apreciar, la base jurídica de esta licitud de los datos se encuentra en el contrato de trabajo, y no tanto en el consentimiento. Esto se debe a que difícilmente se puede aplicar la libertad e incondicionalidad del consentimiento en relaciones de dependencia laboral. La posición de desequilibrio entre la empresa y la persona trabajadora exige extremar las cautelas y, en particular, el respeto a los principios de proporcionalidad y de limitación de la finalidad. (AEPD, 2021)

«Es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas […] Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo. Sin embargo, un interés legítimo en sí mismo no es suficiente para primar sobre los derechos y libertades de los trabajadores» » (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 291)

Cuando, excepcionalmente, la base jurídica del tratamiento sea el consentimiento, éste debe ser inequívoco, de modo que requiere una manifestación del afectado o una clara acción afirmativa, pues el RGPD, a diferencia de la normativa anterior, dispone que el silencio, las casillas ya marcadas o la inacción, no deben constituir consentimiento. (Considerando 32, RGPD)

El consentimiento de las personas trabajadoras, además, debe ser libre y específico, no siendo lícita la sustitución del consentimiento individual por un consentimiento indirecto y plural mediante la negociación colectiva (STJUE, 2014.)

Al trabajador le son enteramente aplicables los principios que el RGPD estableció en su momento, y que la LOGPDDG se ha encargado de actualizar adaptándose a los nuevos tiempos. De forma enumerada y simplificada son los siguientes:

- Derecho de acceso (art. 15 RGPD)

- Derecho de rectificación (art. 16 RGPD)
- Derecho de supresión (art. 17 RGPD)
- Derecho a la limitación de tratamiento (art.18 RGPD)
- Derecho a la portabilidad de los datos (art. 20 RGPD)
- Derecho a la oposición (art. 21 RGPD)
- Derecho a no ser objeto de decisiones individuales automatizadas (art. 22 RGPD)

Hemos visto dos bases jurídicas que habilitan el acceso a los datos de los trabajadores por parte del empresario. Por una parte, la fuerza vinculante del contrato; y por otra y para casos no recogidos, el consentimiento del trabajador y sus garantías. Pasamos a analizar otra circunstancia que licitaría el tratamiento de datos: el interés legítimo del empresario.

Si bien podríamos considerarla como indeterminada y relativa, pues queda en manos del empleador, si que es cierto que esta posibilidad se recoge en el RGPD, en concreto en el artículo 6.1.f). En caso de que un empresario pretenda invocar un interés legítimo la finalidad del tratamiento debe ser legítima; el método elegido o la tecnología específica deben ser necesarios, proporcionados y aplicados de la manera menos intrusiva posible, y el empresario deberá poder demostrar que se han adoptado las medidas adecuadas para garantizar un equilibrio con los derechos y libertades fundamentales de los trabajadores. (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

Una vez determinado las posibilidades que tiene el empresario de acceder a los datos de sus trabajadores, nos ocuparemos de cómo proceder a su tratamiento. El art. 5.b) del RGPD establece que los datos serán "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines" («limitación de la finalidad»); al mismo tiempo que adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos») (art5.c RGPD)

A lo largo de este artículo se recogen los principios relativos al tratamiento de datos personales, si bien nos centraremos en estos dos pues son los que más problemas ocasionan en las relaciones laborales.

1. FINALIDAD DE LOS DATOS

Solo se puede efectuar un tratamiento de datos personales cuando concurre un fin determinado y el tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por el tercero a quien se comuniquen los datos (art 5.b. RGPD). La finalidad por sí sola no justifica el tratamiento de datos, sino que debe ir acompañado de otros principios, ya que es tan genérica y amplia que no supone límite alguno al tratamiento. (Perona, 2021)

Por ello, con carácter previo al tratamiento se hace necesario efectuar una ponderación de los derechos e intereses en conflicto, evaluando las circunstancias concretas del caso particular de que se trate y la importancia de los derechos que la Carta de Derechos Fundamentales de la Unión Europea

Esta finalidad debe de estar determinada al inicio de la relación contractual, de ahí que la AEPD recomiende que se elabore un modelo de "impreso tipo" (fijando un procedimiento de entrega para los candidatos) e informar en dicho impreso del tratamiento de los datos. Y si es el candidato el que presenta directamente el curriculum (por correo electrónico) establecer un procedimiento de obtención y uso de estos datos, incluyendo el acuse de recibo. Respecto al uso de las redes sociales en los procesos de contratación, el GTA 29 en su Dictamen 2/2017 (apartado 5.1) señala que los empleadores pueden creer que inspeccionar los perfiles sociales de los candidatos potenciales está justificado durante sus procesos de contratación.

Sin embargo, los empleadores no deben pensar que, porque el perfil de una persona en las redes sociales está a disposición del público, se les permite procesar esos datos para sus

propios fines. Para que el tratamiento de los datos de los candidatos sea lícito, los empleadores deben cumplir con estos requisitos:

1) Considerar si el perfil del candidato en las redes sociales es privado o público.

2) Recabar y tratar únicamente si es necesario y relevante para el desempeño del puesto de trabajo ofertado.

3) Suprimir los datos personales tan pronto como el candidato sea descartado o rechace la oferta

4) Que el interesado sea informado de dicho tratamiento de datos antes de que participe en el proceso de contratación.

A lo largo de la vida laboral, la finalidad vendrá determinada por las exigencias derivadas del desarrollo de la actividad laboral. Los empleadores solo pueden recopilar datos con fines determinados, explícitos y legítimos.

La concreta finalidad del tratamiento debe estar claramente definida antes del inicio. Puede haber distintos fines, que justifiquen el acceso a los datos personales del trabajador en el lugar de trabajo. Fines que deberán estar explicitados en la política de privacidad de la empresa.

A ello se une la legitimidad, que es otro requisito necesario para la licitud. La finalidad es tan genérica que no supone, como se ha señalado antes, límite alguno, máxime en el ámbito laboral donde fácilmente se tiende a confundir finalidad con cualquier interés del empresario. En la normativa de protección de datos, la determinación del carácter legítimo del fin es condición de licitud del tratamiento. Ello requiere, como se ha señalado antes, efectuar, con carácter previo al tratamiento de datos, una ponderación de los derechos e intereses en conflicto, es decir, determinar qué ha de prevalecer, si el interés del empresario a recabar y tratar datos de los empleados o el respeto a la intimidad de éstos. Para ello se necesita evaluar las circunstancias de cada medida empresarial y de cada caso.

Por lo que respecta, en concreto al control de las comunicaciones electrónicas del empleado, el TEDH entiende, en la Sentencia de 5 de septiembre de 2017 (Asunto, Barbulescu c. Rumania), que no constituye motivo legítimo de acceso a las conversaciones el propósito simplemente de conocer el uso que el empleado hace de los medios facilitados por la empresa, porque se pregunta en la sentencia qué objetivo "pudo justificar una supervisión tan estricta, no habiendo una acusación concreta de actividad ilegal en el espacio virtual que comprometiese a la empresa; de ahí que no reconozca legitimidad a la simple verificación por la empresa del uso personal del servicio de mensajería facilitado al Sr. Barbulescu. Por otra parte, aunque no se menciona en la sentencia la necesidad de indicios fundados, es evidente que el control ofensivo debe estar asentado en sólidos indicios de actividad ilícita, porque el acceso con un propósito meramente preventivo o disuasorio para evitar el uso personal o no consentido de los medios informáticos conduciría a la nada el ejercicio de la vida privada y el secreto sobre el lugar de trabajo

A la hora de determinar la compatibilidad de ese uso posterior con la finalidad de origen, el Reglamento obliga a tener en cuenta los siguientes criterios: a) la relación entre los fines originarios y los fines ulteriores; b) la relación entre los interesados y el responsable del tratamiento c) la naturaleza de los datos personales, en concreto cuando se trate de categorías especiales de datos personales, o datos relativos a condenas e infracciones penales; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Traducido al ámbito laboral significa, como tiene señalado el apartado 6. ("Uso interno de datos") de la Recomendación CM/Rec. (2015) que:

1. Los datos personales recopilados con fines de empleo solo deben ser tratados por los empleadores para tales fines (6.1).

2. Los empleadores deben adoptar políticas, reglas y/u otros instrumentos de protección de datos de uso interno de datos personales de acuerdo con los principios de la Recomendación (6.2).

3. En circunstancias excepcionales, cuando se procesen datos personales sin ser el propósito directo, los empleadores deberán tomar las medidas adecuadas para evitar el uso indebido de los datos para un propósito diferente e informar al empleado (6.3).

2. MINIMIZACION DE DATOS

Ello no implica que el empleador pueda conocer cualquier tipo de dato personal de las personas trabajadoras, porque el principio de minimización de datos exige que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (art. 5 del RGPD).

Sin embargo, otros datos personales no resultan imprescindibles para la ejecución del contrato de trabajo, como, por ejemplo, el nombre de usuario en las redes sociales o en servicios de mensajería o portales de internet. El tratamiento de estos datos por parte del empleador exige la concurrencia de una base jurídica diferente a la ejecución del contrato, como puede ser el interés legítimo, que habrá de demostrarse debidamente atendiendo a los principios de ponderación y proporcionalidad. No obstante, habrá que analizar las características de cada relación laboral para determinar qué datos son necesarios para el cumplimiento de ese contrato y cuáles no. (AEPD, 2021)

Por tanto, el empleador tiene derecho a conocer los datos personales necesarios para el normal desarrollo de la relación laboral, entre ellos, y a título meramente ejemplificativo y no limitativo, los siguientes:

- Nombre y apellidos de la persona trabajadora
- Sexo

- Número de DNI, número de identificación de extranjero y número de afiliación a la Seguridad Social
- Nacionalidad
- Discapacidad
- Fecha de nacimiento

Todos esos datos pueden tener repercusión directa en el cumplimiento de las obligaciones empresariales, por ejemplo, en materia de actos de encuadramiento afiliación, alta y cotización de la Seguridad Social para la comprobación de que la persona trabajadora cumple los requisitos pertinentes para celebrar el contrato entre otros.

Son datos personales los que permiten a la empresa localizar a las personas trabajadoras y contactar con ellas, como el domicilio, la dirección de correo electrónico, el número de teléfono (fijo y/o móvil) o la cuenta bancaria. En general, parece necesario para la ejecución del contrato que el empleador disponga de alguna vía de comunicación con las personas trabajadoras, y es imprescindible que la persona trabajadora proporcione a la empresa alguna forma de contacto. Sin embargo, el contrato de trabajo no legitima a la empresa para solicitar a la persona trabajadora todos esos datos, como ha puesto de manifiesto el Tribunal Supremo en relación con la dirección de correo electrónico o el número de teléfono personal (STS 4086/2015, de 21 de septiembre, Sala de lo Social). Es decir, la necesidad del tratamiento habrá de ponderarse caso a caso. Para ello, será necesario analizar en cada caso la base jurídica alegada –que podría ser el contrato de trabajo, el consentimiento o el interés legítimo del empleador-, la finalidad pretendida y los datos tratados. (AEPD, 2021)

A modo de ejemplo, en relación con el número de cuenta bancaria, se ha venido admitiendo el tratamiento de ese dato personal (Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE del Grupo de Trabajo del Artículo 29). Sin embargo, los principios de minimización

y limitación de la finalidad implican que la empresa únicamente puede proceder a su tratamiento si el salario se abona mediante transferencia, porque debe disponer de los medios a través de los que hacer efectivas las obligaciones correspondientes. En cambio, no podría exigir esa información a las personas trabajadoras cuando el pago se realiza por otra vía que no implique a la entidad bancaria (AEPD, 2021)

Este deber de salvaguardar los datos personales de los trabajadores se extiende hasta que finaliza la relación laboral, incluyendo el momento del despido. El ET exige que se contengan en la carta los hechos que motivan el despido (Art 55), por lo que se podrán incluir todos aquellos datos siempre que sean adecuados y pertinentes para esa finalidad, y no datos personales superfluos o irrelevantes.

En este sentido, así se ha pronunciado la (STS 5138/2005, de 22 de julio, Sala de lo Social) pues no podrán constar en la carta de despido datos personales que el empleador no está legitimado para conocer, máxime cuando se trate de categorías especiales de datos personales, como el diagnóstico médico concreto que motiva un despido por ineptitud.

El derecho a la protección de datos se vería vulnerado en caso de por error, otra persona recibiera esa carta; o se han utilizado datos personales de un tercero para la justificación del despido.

Otro supuesto también lo encontraríamos en el caso de, para justificar nuestro despido, se recojan en la carta de despido datos personales. En este sentido, la Audiencia Nacional (SAN CA 19-10-05). ha admitido la utilización en el proceso judicial de datos relativos a pagos efectuados con la tarjeta de crédito en diferentes peajes aun cuando se correspondían con desplazamientos ajenos al trabajo, en cuanto que servían para tratar de avalar y acreditar los hechos que sustentaban el despido. Según la versión del tribunal, dicha documentación guarda relación con el contrato entre las partes, y más concretamente, con el motivo de extinción de este despido disciplinario.

Si bien señalamos anteriormente que el límite temporal por el que el empresario podría tener acceso a nuestros datos se extingue en el momento de la celebración del despido, ya que la base jurídica de las obligaciones derivadas de un contrato resultaría inoperativa, cabría preguntarse si existen otros motivos que justificarían el acceso aun en el tiempo de extinguirse la relación.

No obstante, esta conclusión es propia, pues ni el RGPD ni la LOPD establecen un plazo concreto de conservación de los datos personales transcurrido el cual los datos tienen que suprimirse. Lo que sí reconocen ambas leyes es el derecho del trabajador a que se supriman sin dilación indebida los datos personales que le conciernan cuando concurran determinadas circunstancias (art. 17 RGPD)

Pues bien, a la finalización de la relación laboral debe procederse al bloqueo de los datos (art. 32 LOPDGDD). No obstante, el tratamiento de datos tras la extinción del contrato podría ser admisible si existe otra base jurídica, como sucederá si el empleador demuestra un interés legítimo. (AEPD, 2021)

Por ejemplo, un empresario respecto de unas personas que ya no forman parte de la empresa, pero sobre las que pesa una cláusula de no competencia. Cabría preguntarse si esta circunstancia podría considerarse como interés legítimo por parte del empleador, y por tanto, habilitarse al acceso de las personas ex trabajadoras.

Pues bien se admite que el empresario pueda seguir conectado a los perfiles de LinkedIn de sus personas extrabajadoras con el fin de controlar el cumplimiento de dichas, siempre que empresario pueda demostrar que dicho control es necesario para proteger sus intereses legítimos; que no existen otros medios menos invasivos; y que las personas extrabajadoras han sido adecuadamente informadas del alcance del control periódico de sus comunicaciones públicas (Dictamen 2/2017 del Grupo de Trabajo del Artículo 29 RGPD).

3.1 DATOS RELACIONADOS CON LA SALUD DURANTE LA COVID19 EN EL AMBITO LABORAL

La base jurídica para habilitar el acceso a esta categoría de datos es distinta a las vistas anteriores. En este sentido, son circunstancias ajenas al contrato de trabajo, al consentimiento y al interés legítimo del trabajador los que hacen posible el tratamiento de los datos relacionados con la salud.

El Tribunal Constitucional (STC 70/2009 de 23 marzo) , hizo hincapié en que, dentro de ese ámbito propio y reservado (íntimo) frente al conocimiento de terceros, se comprende, sin duda, la información relativa a la salud física y psíquica de una persona, que es, además, especialmente sensible y, por tanto, digna de especial protección. Y recuerda la necesidad de que las limitaciones e intromisiones sobre ese derecho sean autorizadas por la ley, de forma precisa y proporcionada. (Timón, 2020)

Pues bien, como norma rectora que es el RGPD, acudiremos a el como hicimos en el anterior apartado para esclarecer que, por razones de interés en el ámbito de la salud pública, el tratamiento de nuestros datos se encontraba habilitado (art.9.2.g RGPD). Pues bien, es en la letra B del mismo artículo es donde aparece otra excepción a la prohibición del tratamiento de nuestros datos, y que guardan una íntima relación con lo que nos vamos a ocupar: el tratamiento de nuestros datos estará permitido cuando sea necesario para el cumplimiento de obligaciones y ejercicios específicos del responsable del tratamiento en el ámbito del derecho laboral; para añadir que, estará autorizado por el derecho el Estado Miembro en cuestión, responsable de dictar las garantías adecuadas del respeto de derechos fundamentales y de los intereses del interesado. (art. 9.b RGPD)

Asimismo, el art. 9.2 .h) del RGPD admite la recogida y tratamiento de datos con fines de «medicina preventiva o laboral» y «evaluación de la capacidad laboral del trabajador», sin perjuicio de que han de respetarse las garantías y límites pertinentes en relación con los datos que se pretenden obtener y su posible uso posterior.

La LPRL y sus normas de desarrollo imponen a la empresa la realización de un conjunto de actividades cuyo fin último es evitar o disminuir los riesgos derivados del trabajo. Para esta tarea resulta necesario tratar datos personales de las personas trabajadoras. El tratamiento de datos personales en materia de prevención de riesgos se encuentra legitimado por la existencia de una relación contractual cuyo cumplimiento, desarrollo y control lo hace necesario. El contrato de trabajo, en combinación con el cumplimiento de las obligaciones legales establecidas en el ET y en la LPRL, son las bases jurídicas del tratamiento de datos.

Una de las obligaciones principales del empleador en el campo de la prevención de riesgos laborales es la vigilancia en la salud de las personas trabajadoras. Es una obligación que no implica un deber correlativo para las personas trabajadoras, pues los reconocimientos médicos a cargo del empleador son, con carácter general, voluntarios para aquéllas, que deben prestar su consentimiento. (Art. 14 LPRL)

Esta vigilancia de la salud puede ser obligatoria conforme al artículo 22.1 de la LPRL, previo informe de los representantes de las personas trabajadoras, en los siguientes supuestos:

Reconocimientos imprescindibles para evaluar los efectos de las condiciones de trabajo sobre la salud de las personas trabajadoras.

Verificación de si el estado de salud de la persona trabajadora puede constituir un peligro para ella misma, para las demás personas trabajadoras, o para otras relacionadas con la empresa.

Obligación legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

Tanto si el reconocimiento médico es voluntario como si es obligatorio, la base jurídica para el tratamiento de datos personales derivados de esa vigilancia de la salud no sería el consentimiento, sino la ejecución del contrato de trabajo (art. 6.1.b) del RGPD) y el cumplimiento de las obligaciones legales en materia de prevención, como se ha indicado.

Refiriéndonos a la materia estrictamente relacionada con la COVID19 una de las primeras cuestiones que se nos suscita es si estoy obligado a comunicar a la empresa a la que presto servicios si he dado positivo, y, en caso afirmativo, en qué medida la privacidad de estos datos se encuentra garantizada.

Buscamos una respuesta legal y jurídica, puesto que éticamente la respuesta en todo caso sería afirmativa, a fin de evitar la propagación del virus. Pues bien, ya en el Real Decreto 2210/1995 de 28 de diciembre por el que se crea la red nacional de vigilancia epidemiológica se recogen una serie de enfermedades, que, conforme al artículo 9, son de declaración obligatoria a las autoridades sanitarias. Ha sido a través del Real Decreto-Ley 21/2020 de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19 la que normativiza en su artículo 22 que el contagio por la COVID19 será de declaración obligatoria.

No obstante, recordamos que los receptores de esta información son las Entidades Públicas y sanitarias encargadas de la prevención del coronavirus. En cualquier caso, podríamos considerar esta circunstancia como de comunicación obligada tanto al empresario como a sus compañeros, atendiendo a los deberes que la LPRL impone a los trabajadores en su artículo 29.2.4º[6]

---

[6] 2. Los trabajadores, con arreglo a su formación y siguiendo las instrucciones del empresario, deberán en particular:

1.º Usar adecuadamente, de acuerdo con su naturaleza y los riesgos previsibles, las máquinas, aparatos, herramientas, sustancias peligrosas, equipos de transporte y, en general, cualesquiera otros medios con los que desarrollen su actividad.

2.º Utilizar correctamente los medios y equipos de protección facilitados por el empresario, de acuerdo con las instrucciones recibidas de éste.

Hemos dejado sentado que la comunicación de haber sido contagiado por la COVID19 o tener síntomas es una obligación que el trabajador debe cumplir. En consecuencia, cabría preguntarse qué consecuencias tiene su negativa. Pues bien, es el apartado 3 del mismo artículo el que, ante dicho incumplimiento faculta al empleador a la imposición de sanciones en virtud de falta muy grave, grave o leve, atendiendo a su gravedad, pudiéndose llegar al extremo de que el trabajador sea despedido. Aunque se reserve a los casos más extremos, podría defenderse su procedencia.

Por otra parte, también cabría cuestionarse el grado de responsabilidad que tiene el empresario. En caso de que un empleado se contagie de coronavirus por actitud irresponsable y ponga en riesgo a sus compañeros, se podría ponderar el grado de culpas, en el sentido de que el empleador también podría haber tomado cautelas como hacer PCR a sus trabajadores o controlarles la temperatura, medidas que podrían haber evitado el contagio de otros trabajadores.

Esta consideración deviene de la propia LPRL, la cual en su artículo 22 obliga al empresario a garantizar a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo siempre que lo hagan con proporcionalidad

3.º No poner fuera de funcionamiento y utilizar correctamente los dispositivos de seguridad existentes o que se instalen en los medios relacionados con su actividad o en los lugares de trabajo en los que ésta tenga lugar.

4.º Informar de inmediato a su superior jerárquico directo, y a los trabajadores designados para realizar actividades de protección y de prevención o, en su caso, al servicio de prevención, acerca de cualquier situación que, a su juicio, entrañe, por motivos razonables, un riesgo para la seguridad y la salud de los trabajadores.

5.º Contribuir al cumplimiento de las obligaciones establecidas por la autoridad competente con el fin de proteger la seguridad y la salud de los trabajadores en el trabajo.

6.º Cooperar con el empresario para que éste pueda garantizar unas condiciones de trabajo que sean seguras y no entrañen riesgos para la seguridad y la salud de los trabajadores.

y de acuerdo con las pautas dadas por las autoridades sanitarias y su servicio de prevención de riesgos laborales y vigilancia de la salud.

Esta información puede obtenerse a través de preguntas al personal, pero dichas preguntas solo deberán limitarse a indagar sobre la existencia de síntomas o si el trabajador ha sido diagnosticado como contagiado o sujeto a cuarentena, de manera que no deben usarse cuestionarios de salud extensos y detallados o que incluyan preguntas no relacionadas con la enfermedad (Beloki, 2021) en consonancia con los principios de la limitación de la finalidad y minimización de datos vistos anteriormente.

La figura del consentimiento del trabajador también es difusa, pues es el último artículo citado (art.22 LPRL) el que, atendiendo a las circunstancias, lo considera obligatorio o no. Excluye la voluntariedad en

"(…)los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad."

por lo que atendiendo al ritmo de contagios que la COVID19 ha tenido durante esta pandemia, se considera exceptuado el consentimiento.

Por lo tanto, estaríamos en una situación perfectamente legal que, la empresa, en cumplimiento de la LPRL realice un control de temperatura sin nuestro consentimiento, dando como resultado unas temperaturas compatibles con la COVID19 y nos tengamos que ausentar del trabajo por motivos de precaución. Misma situación llegaríamos si el trabajador, en

cumplimiento con su cuota de obligación que la misma LPRL le impone en estas circunstancias, ha sido el que ha declarado su contagio ante su superior.

Sea como fuere, la empresa ha tenido acceso a nuestros datos, por lo que estudiaremos las posibilidades que tiene respecto de su tratamiento. El empresario se encuentra en una situación en la que debe proteger la salud del resto de trabajadores, por lo que su comunicación a todos ellos resulta necesaria. Esta información debería proporcionarse sin identificar a la persona afectada a fin de mantener su privacidad, si bien, podría transmitirse a requerimiento de las autoridades competentes, en particular las sanitarias.

La información debe proporcionarse respetando los principios de finalidad y proporcionalidad y siempre dentro de lo establecido en las recomendaciones o instrucciones emitidas por las autoridades competentes, en particular las sanitarias. Por ejemplo, si es posible alcanzar la finalidad de protección de la salud del personal divulgando la existencia de un contagio, pero sin especificar la identidad de la persona contagiada, debería procederse de ese modo. Si, por el contrario, ese objetivo no puede conseguirse con información parcial, o la práctica es desaconsejada por las autoridades competentes, en particular las sanitarias, podría proporcionarse la información identificativa. (AEPD, 2021)

Siguiendo con nuestro supuesto, y mencionando a una de las modalidades de trabajo que más se ha repetido durante y posterior a la pandemia como es la figura del teletrabajo, analizaremos la incidencia que ha podido tener en el derecho a la protección de datos.

En cualquier caso, la necesidad y la obligatoriedad del cumplimiento de la normativa sobre protección de datos personales persiste cualquiera que sea la modalidad de trabajo, por lo que los diferentes organismos y entidades han de establecer, también en el caso del 'teletrabajo', las medidas técnicas y organizativas necesarias con vistas a garantizar la seguridad en la utilización de los sistemas informáticos y en el tratamiento de los datos personales.

Atendiendo a lo visto anteriormente, y en cumplimiento con el RGPD, la LPRL y todo lo relativo a la protección de datos, a modo de conclusión, estas serían algunas de las actuaciones que podrían tomar los empleadores:

- Informar a los trabajadores de su obligación de notificar al empresario en caso de presentar síntomas del coronavirus a fin de preservar su propia salud y evitar el contagio al resto de compañeros y ciudadanos
- Elaborar y enviar un breve cuestionario para saber el estado de salud de los trabajadores y a partir del mismo adoptar las medidas preventivas necesarias en cumplimiento de la ley. En este cuestionario se podrá formular preguntas para verificar si el trabajador está infectado o no, o saber si ha visitado algún lugar de riesgo de infección en las últimas semanas, entre otras. En todo caso, se prohíben cuestionarios de salud extensos y detallados o que incluyan preguntas no relacionadas con la infección del virus.
- Guardar la información recopilada del cuestionario durante el tiempo estrictamente necesario y para la finalidad concreta. Se deberá garantizar en cualquier caso la privacidad del trabajador, incluso a nivel interno, y salvo requerimiento por parte de las autoridades competentes (por ejemplo, la autoridad sanitaria).

4. **CONCLUSIONES**

I. El derecho a la protección de datos, como lo conocemos hoy en día, ha sufrido un largo proceso de transformación y renovación. Esta actualización en cuanto a su contenido no va sino a seguir sucediéndose en las generaciones venideras. A pesar de ello, la normativa que dicta las bases para su desarrollo es principalmente europea, a cuyas actuaciones se siguen sometiendo los sujetos que tienen acceso a nuestros datos.

II. Este derecho no protege a la persona sino a los datos que la identifican; al mismo tiempo que no trata de impedir el acceso a nuestros datos, sino más bien como deben ser tratados. La protección de datos no es un derecho impertinente que "prohíba" sin más "hacer cosas"; más bien marca el camino que indica "cómo deben hacerse las cosas".

III. Este modo de proceder con nuestros datos estará condicionado por las circunstancias concretas en cada caso, entendidas como bases jurídicas. El tratamiento de nuestros datos deberá tener una base jurídica que lo respalde, y, como hemos visto, son de diversa naturaleza: ejecución de un contrato, cumplimiento de obligaciones legales o preservar la salud pública.

IV. Estos tres ejemplos de bases jurídicas son las que han justificado el tratamiento de nuestros datos en la línea de esta investigación. Por ello, y en consonancia con el interés de la salud pública, entendida como evitar la propagación de la pandemia, se puede concluir que la COVID19 no ha supuesto un marco excepcional ni para el tratamiento de nuestros datos, ni para el ejercicio de nuestros derechos.

V. La normativa sigue estando vigente en todo momento, no habiendo tenido ningún efecto la limitación de otros derechos respecto del que nos ha tocado investigar. Por lo tanto, el análisis de su legitimidad devendrá de la concordancia de las actuaciones llevadas a cabo con la normativa que lo regula. Se ha podido comprobar como en nuestro país se han encontrado deficiencias que ha puesto en juego la privacidad de nuestros datos (app RADAR COVID19).

VI. Por último, han sido los otros dos ejemplos de bases jurídicas: ejecución de un contrato y cumplimiento de obligaciones legales los que han justificado el tratamiento de nuestros datos en el ámbito laboral, teniendo especial significación la figura del consentimiento, dada la naturaleza de la relación. El interés legítimo del empleador permite que incluso se extienda el tratamiento de nuestros datos aun habiéndose extinguido la relación laboral.

VII. Estamos ante una normativa no estanca y flexible abierta a muchas posibilidades, lo que también exige un buen manual de instrucciones a las empresas respecto de los datos de sus empleados para no vulnerar su derecho a la protección de datos, y de especial relevancia, los datos relativos a la salud durante la COVID19. En él hemos comprobado que el deber de preservar la salud pública resulta prioritario en todo momento, si bien los datos del trabajador deben ser tratados bajos los principios de finalidad y minimización a fin de que no se pierda su anonimato.

VIII. En definitiva, habiéndose enfrentado el derecho fundamental a la protección de datos con la obligación ética y legal de preservar la salud pública, ha quedado claro que debe primar el segundo teniendo en cuenta el carácter colectivo de este. Es la normativa reguladora de este derecho la que garantiza que su tratamiento no va a ser indiscriminado, sin que pueda torpedear las actuaciones para evitar la

propagación del virus, pues cuando ponderamos los derechos individuales frente a los colectivos, cuando esgrimimos los derechos fundamentales como absolutos, no hacemos más que ir en contra del interés colectivo, y, en consecuencia, del nuestro propio.

5. BIBLIOGRAFÍA

Burkert, H. (2000). *Privacy -- Data Protection. A German/European Perspective.* St Gallen: Nomos Verlagsgesellschaft .

Cruz, P. (1989). Formación y evolución de los derechos fundamentales. *Revista Española de Derecho Constitucional* , 41.

Douwe, K., & Maria, G. (2019). *Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del.* Bruselas: El Manual del DPD.

Fernandez, J. M. (2003). El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario. *XI Congreso de Derecho y Salud : "Nuevos retos del Sistema Nacional de Salud"*, 37-46.

Fernandez, S. (22 de Octubre de 2020). La 'app' Radar COVID registra una brecha de seguridad que vulnera la privacidad de los usuarios. *CADENASER.COM*.

Lorenzo, M., & Reyes, C. G. (2002). EL ORDENAMIENTO ESPAÑOL Y LA PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR DE LAS TELECOMUNICACIONES. *Boletines del Ministerio de Justicia*, 3565-3583.

Márquez, C., & Ortega, J. A. (2020). La COVID-19 y los desafíos de la vigilancia digital para los derechos humanos: a propósito de la app DataCOVID prevista en la Orden Ministerial SND/29/2020, de 27 de marzo. *Bioética y Derecho*, (50), 205-220. Epub 23 de noviembre de 2020.

Martinez, R. (2021). Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. *Diariolaley*.

Pascual, P. (2017). *La génesis del derecho fundamental a la protección de datos.* Universidad Complutense de Madrid: Tesis Doctoral.

Pérez, J. (22 de Octubre de 2020). La ‘app’ Radar Covid ha tenido una brecha de seguridad desde su lanzamiento. *EL PAIS*.

Piñar, J. L. (Marzo de 2020). La protección de datos durante la crisis del coronavirus. *abogacia.es*.

Saldaña, M. N. (2012). «The right to privacy»: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis. *Revista De Derecho Político*, 195-239.

Timón, M. (2020). *Protección de datos de carácter personal y crisis sanitaria (Covid 19).* Lefebvre.

Warren, S., & Brandeis, L. D. (1890). *The right to privacy.* Boston: Outlook Verlag.

ANEXOS

- ANEXO I: RECLAMACION ANTE LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS (7 DE SEPTIEMBRE DE 2020)

RECLAMACION APP RADAR COVID.pdf

- ANEXO II: AMPLIACION DE LA RECLAMACION ANTE LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS (24 DE ENERO DE 2021

AMPLIACION RECLAMACION APP