Facultad de Ciencias Sociales y Jurídicas

Grado en Derecho

Universidad de Jaén

Facultad de Ciencias Sociales y Jurídicas

Trabajo Fin de Grado

# PROTECCIÓN DE DATOS: EVOLUCIÓN, ACTUALIDAD, ANÁLISIS Y LA INFLUENCIA DEL COVID-19.

**Alumno: David Rivas Castillo.**

**Julio, 2020**

PROTECCIÓN DE DATOS: EVOLUCIÓN, ACTUALIDAD, ANÁLISIS Y LA INFLUENCIA DEL COVID-19.

ÍNDICE

**RESUMEN.**

El tema elegido "PROTECCIÓN DE DATOS: EVOLUCIÓN, ACTUALIDAD, ANÁLISIS Y LA INFLUENCIA DEL COVID-19*"*, deriva de la intención de elaborar un estudio sobre los hechos históricos y normativos de relevancia jurídica que han dado forma a lo que hoy día conocemos como protección de datos y la repercusión que el estado de alarma ha supuesto en la forma de manejar datos de carácter personalísimo y su libre circulación.

**ABSTRACT.**

The aim of this project, "DATA PROTECTION: EVOLUTION, TOPICALITY, ANALYSIS AND INFLUENCE OF COVID-19", is to elaborate a study on the legally-relevant historical and law facts that have shaped what we know as data protection. In addition, thorough this research I will analyse the implication of the state of alert in the way of managing personal data and its free movement.

## 1. INTRODUCCIÓN.

El siguiente trabajo se encuadra en la Rama de Derecho Constitucional, bajo el tema "PROTECCIÓN DE DATOS: EVOLUCIÓN, ACTUALIDAD, ANÁLISIS Y LA INFLUENCIA DEL COVID-19*"*. La evolución que ha supuesto la protección de datos personales ha surgido como respuesta al avance de la informática durante estas últimas décadas, ya que en el contexto de la sociedad globalizada y cada vez más digitalizada en la que vivimos, la utilización de las Tecnologías de la Información y de la Comunicación (TIC) ha supuesto un cambio drástico en la forma de desarrollar las labores en el mundo. Es por ello que la protección de datos, que se ubica dentro del campo de estudio del derecho informático y su desarrollo de estas materias, ha sido elaborado en un tiempo récord.

Para las leyes reguladoras y la jurisprudencia a día de hoy, cualquier ciudadano tiene derecho a la protección de datos, suponiendo un amplio espectro de facultades tales como la

que rodea a la propia figura personal del ciudadano, hablamos de los datos personales del mismo, así como su posterior tratamiento. De esta manera, se entiende por dicha protección de datos, cualquier dato por el cual a través de este se identifica o se haga alusión de manera directa o indirecta a una persona física, es decir, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

Cabe destacar, antes de cualquier posible análisis sobre las distintas normas que han surgido, que estas van dirigidas a regular la utilización y tratamiento de los datos personales, por lo que se pretende proteger y asegurar los derechos propios de la persona a la que se refieren los datos.

Respecto al origen que regula la protección de datos a nivel europeo, no existen grandes diferencias entre las leyes de los distintos Estados Miembros, ya que todas ellas han tomado como referente el CEDH (Convenio Europeo de Derechos Humanos) y la jurisprudencia del TEDH (Tribunal Europeo de Derecho Humanos). De igual manera ocurre actualmente, basándose las normativas al respecto en el RGPD (Reglamento General de Protección de Datos).

Todos los estados europeos han considerado que el objeto del derecho a la protección de datos personales es garantizar al individuo el derecho a organizar y determinar por sí mismo aspectos esenciales de su vida, es decir, que el fundamento último de este derecho es la dignidad de la persona.

Por lo tanto, se expondrá en primer lugar un marco general normativo en relación con el origen y la evolución de la protección de datos en España, además de los correspondientes comentarios a la regulación que fuera necesaria por parte de la Unión Europea, destacando que, de entre todo ello, en el ámbito de la Constitución Española (CE), se otorga a todos los ciudadanos una serie de derechos fundamentales y libertades públicas. Es a través de la Constitución de 1978, concretamente en su artículo 18, donde el derecho español fundamenta el peso, la necesidad y la obligación de la defensa y regulación de la protección de datos de cara a la seguridad del honor e intimidad personal de los ciudadanos.

En España, se regula por primera vez los medios informáticos que influyen en la garantía de la intimidad personal con la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), que desarrolla el contenido del artículo 18 de la CE.

Tras esto, se promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que vino a adaptar la legislación europea, incluyendo, los datos de carácter personal registrados en soporte físico y toda modalidad de uso de los mismos.

Con posterioridad a la LOPD, se introdujo el Real Decreto 1720/2007, que de manera sintetizada y a grandes rasgos, venía a realizar un desarrollo normativo mucho más extenso y complementario de la LOPD. Este decreto introducía la idea de tres diferentes niveles de seguridad, clasificados en función de la garantía que se pretendiera cubrir con ellas.

Llegando a la regulación europea vigente nos encontramos con lo que fue el desarrollo del Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 Europeo de Protección de Datos (RGPD) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Dicho reglamento realiza un nuevo marco cuyo análisis estará versado sobre privacidad, el deber de información, el consentimiento, la transparencia y la seguridad, que se convertirían en los principales principios y derechos reguladores del tratamiento de datos personales en materia de protección de datos.

Es con el desarrollo del RGPD, de obligado cumplimiento para los Estados miembros, que España adapta el Reglamento dando lugar a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), siendo así el primer Estado miembro que adaptó el Reglamento, pero con el añadido de ciertas novedades. Algunos de los cambios más significativos que realizó el LOPDGDD respecto del RGPD fue el cambio de edad en el menor para que este pueda otorgar consentimiento sobre los mismos y el hecho de que los familiares puedan solicitar la protección de datos de las personas fallecidas.

También, cabe destacar como figura de vital importancia en la protección de datos en España la figura de la Agencia Española de Protección de Datos (AEPD) como órgano de gran relevancia por ser el encargado de controlar la aplicación correcta de la ley vigente y la encargada de sancionar para los casos en los que fuera necesario.

Y, por último, el correspondiente análisis por la declaración del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, proclamándose como primera crisis sanitaria en España ante la situación de pandemia provocada y la correlativa aplicación en base a esta por lo regulado en la LOPDGDD y la RGPD en garantía de salvaguardar el derecho a la protección de datos ante una situación excepcional.

## 2. LEY ORGÁNICA DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL (LORTAD).

El primer atisbo sobre la protección de datos en España surge con la CE de 1978 mediante dos preceptos básicos regulado en el Capítulo II, Sección l. «De los derechos fundamentales y de las libertades públicas», en los artículos 16 y 18. Dichos artículos, en concreto el 18, si lo entendemos textualmente, no habla de «regular», sino de «limitar», de manera que puede suponerse que la disposición de la CE en origen era negativa respecto de la utilización de la informática.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) fue la primera norma en materia de protección de datos que fue aprobada en España. Posteriormente, tras su publicación y entrada en vigor, la LORTAD fue modificada y complementada por el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal; y el Real Decreto 994/1999, de 11 de junio, sobre medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. En la actualidad se encuentran derogadas, pero en su periodo de vigencia, la LORTAD venía a cubrir la necesidad de un sistema de garantías y medidas cautelares. Su creación surgió como necesidad de adaptar el artículo 18.4 de la Constitución Española, ya nombrado anteriormente, y el artículo 4 del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Respecto de la regulación de esta norma encontramos que está integrada por una Exposición de Motivos, 48 artículos distribuidos en 7 Títulos, 3 disposiciones adicionales, una disposición transitoria, una disposición derogatoria y 4 disposiciones finales.

Con la entrada en vigor de la LORTAD surgió como parte de su contenido la figura de la Agencia de Protección de Datos, que más tarde con la posterior regulación sobre materia de protección de datos pasaría a denominarse Agencia Española de Protección de Datos

En definitiva, la LORTAD se estableció como una regulación pionera a nivel nacional tratando temas de diferentes índoles como: la definición de los principios básicos sobre

protección de datos, y el reconocimiento y tutela jurídica de la libertad informática, además de las primeras pinceladas sobre los principios relativos al tratamiento de los datos personales.

## 3. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD).

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que se encuentra actualmente derogada por la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantías de los Derechos Digitales (LOPDPGDD), que adapta el Reglamento General de Protección de Datos de la Unión Europea (RGPD), fue la primera ley orgánica española en adaptar la legislación europea con el objetivo de asegurar y garantizar los datos personales y libertades públicas, concretamente la seguridad del honor e intimidad de los ciudadanos. Al igual que ocurría con su predecesora, la LORTAD, esta desarrolla el artículo 18 de la CE.

La LOPD fue fruto de la transposición de la Directiva 95/46, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.

Dentro encontramos un articulado, por el cual se asegura, como ya hemos dicho, la protección de ciertos datos de carácter personal, que vienen a clasificarse en función de su mayor o menor grado de protección, surgiendo así una mayor restricción en base a su protección jurídica y apoyándose en caso de que fuera necesario en la AEPD, que será el órgano de control encargado para el caso de incumplimiento de la norma de dar ciertas resoluciones para velar por el cumplimiento de esta.

Estableció en cuanto al consentimiento que este aplicaba, en su artículo 6, una explicación sobre la importancia del requerimiento de consentimiento inequívoco de la persona afectada, que podrá ser revocado si existiera alguna causa justificada. Además, en función de los datos de carácter personal a tratar se clasificó entre diferentes tipos de consentimiento, distinguiendo entre consentimiento inequívoco cuando fuera exigido por el carácter de importancia que represente y tácito para cuando no fuera exigido un consentimiento expreso. Cualquiera que diera su consentimiento para el tráfico de sus datos tendría la posibilidad de revocarlo y aquel

al que le hubieran sido otorgados los mismos estaría desde ese momento a disposición de lo presente en la ley.

Para el caso de que un tercero tuviera acceso a los datos este debía hacer constar su uso en un contrato, estableciéndose en el mismo que usará los datos ateniéndose a un uso responsable del mismo y para lo acreditado en el contrato con carácter exclusivo. Cabe destacar que se permitía el tratamiento de datos sin necesaria comunicación inmediata, otorgando un plazo de tres meses para hacerlo e incluso la no comunicación en ese plazo para los casos de que la información fuera accesible al público, cuando esté autorizada por ley, entre otras excepciones.

La LOPD establecía en cuanto al deber de información en su artículo 5, la obligación de informar y facilitar datos, por lo que debía asegurarse mediante los medios previstos con el previo consentimiento y, para el tratamiento sobre la comunicación de los datos, es preciso remarcar que no solo las personas jurídicas sino cualquier persona tendría acceso para realizar consultas.

## 4. REGLAMENTO 1720/2007 DE DESARROLLO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS.

Con la aparición del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, como ya se introdujo anteriormente la idea, se dio lugar a una modificación sustancial de la LOPD, que venía a realizar un desarrollo normativo mucho más extenso y complementario como necesidad del avance tecnológico como es costumbre en este tipo concreto de leyes. Al igual que ocurría con la LOPD, se encuentra parcialmente derogada para todo aquello que implicara alguna contradicción o aplicara diferentes tratamientos y resolución respecto a la actual regulación actual de la LOPDGDD, prevaleciendo esta última. De esta manera y como mayor característica a destacar de la misma, se venía a introducir tres diferentes niveles de seguridad dependiendo de la naturaleza de los datos, por lo que su clasificación fue en función de la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Estos tres diferentes niveles de seguridad respecto de las medidas eran de obligado cumplimiento y se clasificaban de la siguiente manera:

a) Medidas de nivel básico: Estas medidas pertenecen y son de aplicación a cualquier fichero que contuviera cualquier dato de carácter personal. Por dicho tipo de datos se hace alusión a aquellos relativos a la salud, datos sobre ideología, religión, origen racial, sexualidad, etc.
b) Medidas de nivel medio: Para este rango, los datos personales a tratar hacen referencia a información sobre infracción administrativas o penales, servicios financieros y de gestión tributaria, servicios comunes de la Seguridad Social y cualquier dato que pudiera dar cabida a un perfil que permita la definición de los aspectos personales de un ciudadano. Se incluyen además todos los datos pertenecientes al nivel anterior.
c) Medidas de nivel alto: Recoge tanto los datos personales del nivel medio como el básico, con el añadido extra de datos de especial protección, citados en el nivel básico, y cualquier dato que tuviera un fin policial.

## 5. REGLAMENTO GENERAL DE PROTECCION DE DATOS (RGPD).

Finalmente, habiendo llegado al marco actual vigente a nivel europeo sobre protección de datos, es importante destacar y analizar la llegada del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), que como ya se ha reiterado de manera sucesiva en ideas anteriores, surge de la necesidad de adaptar y regular la privacidad y la protección de datos debido a la evolución de las nuevas tecnologías. Fue aprobada en 2016, pero no fue hasta 2018 que se aplicó, de esta manera en 2018 entró en vigor el RGPD como normativa europea de obligatoria implementación que derogaba parcialmente a la LOPD y al Reglamento 2007 en todo lo que contraviniera a esta.

Este novedoso reglamento ofrece una protección de las personas físicas cuyo fundamento es el tratamiento de datos personales y a la libre circulación de estos datos.

El objetivo del RGPD es el nuevo marco que ha surgido en torno a la privacidad, el deber de información, el consentimiento, la transparencia y la seguridad. Es en torno a este

marco que surgen nuevos derechos que deben prestarse a los usuarios. En relación con su ámbito de aplicación, se establecen dos distinciones:

a) Un ámbito de aplicación material regulado en el artículo 2 donde se plasma la determinación en cuanto que será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
b) Y un ámbito territorial en su artículo 3 donde se matiza la aplicación al tratamiento de datos personales, es decir la aplicación del RGPD, a organizaciones no europeas siempre que tuvieran por cualquier medio trato con la misma.

De esta manera, el RGPD se presenta como un nuevo marco normativo actualizado y, derivado de esa misma actualización, surgen unas principales novedades relativas al tratamiento de datos y condiciones de consentimiento, la regulación del derecho de supresión de los datos personales conocido como el derecho al olvido, derecho a la portabilidad de datos para la figura del interesado, la responsabilidad del responsable del tratamiento en vistas de garantizar mediante medidas que el tratamiento es conforme al Reglamento, notificación para el caso de una violación de la seguridad de los datos personales a la autoridad de control y la regulación de las transferencias internacionales de datos junto con la cooperación entre autoridades de control.

Añade en uno de sus primeros artículos, el artículo 4 concretamente, un glosario de definiciones de los conceptos de carácter esencial sobre la regulación de la protección de datos de carácter personal en post de desglosar y acercar al interesado un mínimo necesario para conocer el alcance de los derechos del RGPD y su cumplimiento.

Por nombrar una de las novedades que este reglamento viene a aportar podemos nombrar a la obligación de establecer una Autoridad de Supervisión (SA), obligando a cada estado miembro que conste de un órgano de este tipo. La labor de este órgano es similar a la que ejercita la AEPD en España, es decir, velar por el cumplimiento de la ley vigente sobre protección de datos y de controlar su aplicación, además de promover sanciones si fuera necesario.

Otra novedad del reglamento es respecto al tratamiento de datos de menores, ya que la UE ha dispuesto que los menores puedan prestar capacidad en el consentimiento respecto de datos personales que les incumbiera directamente. Para ello se ha dispuesto como regla que los menores deben tener mínimo 16 años para prestar ese consentimiento, pero a su vez se le otorga

a los Estados miembro la posibilidad de establecer su propio límite, siempre que este no fuera inferior a los 13 años.

### 5.1. Delegado de protección de datos.

Una de las principales novedades que implicó el Reglamento es la creación de la figura del Delegado de Protección de Datos, también llamado controlador de datos, pues es el encargado del tratamiento de los datos de tal manera que supervisa el obligatorio cumplimiento del Reglamento, pero con el énfasis de que lo hace de cara a la entidad o empresa para la cual ha sido contratado.

El nombramiento que corresponda a una persona en esta posición deberá comunicarse a la Agencia Española de Protección de Datos al ser la autoridad encargada del control del cumplimiento de la legislación sobre protección de datos.

### 5.2. Sistema de proactividad en materia de protección de datos.

La nueva legislación europea sobre protección de los derechos y libertades de las personas físicas, es decir, el RGPD, introduce respecto a los tratamientos de datos personales un principio que se encuentra recogido en el artículo 5.2 y 24, así como en el Considerando 74, en materia de responsabilidad, cuya extensión engloba a instituciones y organizaciones con el fin del cumplimiento del mismo.

El principio de Responsabilidad Proactiva o Accountability introducido se traduce como una obligación impuesta a los responsables del tratamiento de datos para el cumplimiento de la normativa de protección de datos mediante medidas y técnicas organizativas, que deben ser revisadas y actualizadas.

Los responsables de los tratamientos de datos deberán de ser capaces de adecuar las exigencias del RGPD a las operaciones o medidas que se estimen convenientes para su tratamiento.

## 6. LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES (LOPDGDD).

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) se trata de la legislación vigente a nivel nacional sobre materia de protección de datos y se constituye como una asimilación y adaptación del RGPD al marco legislativo español. Dicha normativa entró en vigor en diciembre de 2018, aprobada por las Cortes, siendo así el primer Estado miembro que adaptó el Reglamento, añadiendo ciertas novedades.

Por razones obvias, al tratarse de una adaptación de un reglamento europeo, al igual que ocurría con el mismo, busca adaptar y regular el consentimiento, la privacidad y la protección de datos debido a la evolución de las nuevas tecnologías.

Una de las principales novedades propias de la LOPDGDD respecto del RGPD ha sido la capacidad para solicitar la protección de datos en su artículo 3 por parte de los familiares de personas fallecidas, que será objeto de análisis más adelante.

Por otra parte, y volviendo al tema del tratamiento de los datos personales del individuo, en la LOPDGDD se recoge que las personas tendrán el derecho a saber quién será el responsable del uso de su información, además, se le otorga a la persona la posibilidad de tener un acceso temprano y escueto a los datos que serán utilizados. Otras novedades que han sido incluidas con respecto a sus predecesoras han sido tales como el derecho de acceso, el consentimiento de menores y el bloqueo de datos.

El ámbito de aplicación de la LOPDGDD vendrá establecido en los Título I a IX, que será aplicable a cualquier tratamiento de datos personales contenidos o destinados a ser incluidos en un fichero, ya sea total o parcialmente automatizado, así como no automatizado, con las correspondientes excepciones.

Cabe destacar especialmente algunos títulos y articulado dentro de la propia ley, de los cuales algunos han sido trascritos de forma literal a los del propio reglamento y otros se tratan de añadidos regulados especialmente para el caso de España. Estos últimos son:

a) En el Título VII, referido a las “Autoridades de protección de datos” se hace alusión a la Agencia Española de Protección de Datos y a las Autoridades autonómicas de protección de datos.

b) En el Título X, regulado en los artículos 79 a 97 se regula la *"Garantía de los derechos digitales"*, algunos de ellos son tales como el derecho de acceso universal, neutral y seguro a internet, derecho a la educación digital, derecho de rectificación, actualización y olvido en internet, etc., con la idea de *"que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital"* (párrafo tercero el considerando IV de la LOPDGDD)

El añadido de un Título dedicado a la carta de derechos digitales dentro de la ley española supone una medida pionera por ser la primera de esta naturaleza a nivel comunitario. Dentro de estos derechos, la LOPDGDD hace una doble distinción entre derechos digitales de carácter personal y aquellos que afectan a las personas en el ámbito laboral.

## 7. LA AGENCIA ESPAÑOLA DE PROTECIÓN DE DATOS (AEPD).

La Agencia Española de Protección de Datos es el órgano de control encargado del cumplimiento de la normativa española vigente de protección de datos, es decir, de velar por el cumplimiento de esta y de controlar su aplicación con el objetivo de garantizar los derechos fundamentales sobre datos de los ciudadanos. Fue creada en 1994 conforme a lo establecido en la derogada LORTAD de 1992.

Es un órgano constituido como ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de la Administración pública en el ejercicio de sus funciones. La AEPD tendrá la potestad para actuar tanto a instancia del ciudadano como de oficio, además, es estatutaria y jerárquicamente independiente y se relaciona con el Gobierno a través del Ministerio de Justicia. La misma AEPD otorga a disposición de los ciudadanos una página web oficial con el objetivo de fomentar que conozcan sus derechos y las posibilidades que se les ofrece para ejercerlos.

La AEPD cumple unas funciones establecidas y entre algunas de ellas se pueden distinguir:

a) Como ya ha sido citado anteriormente, velar por el cumplimiento de la normativa vigente de protección de datos, en especial en lo relativo a los

derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) La tutela y cooperación con organismos internacionales en post del control y cumplimiento en materia de protección de datos.
c) Entre otras funciones podemos encontrar la potestad sancionadora, así como la atención de las peticiones y reclamaciones realizadas por los afectados respecto a su tratamiento e información de derechos.

## 8. FIGURAS Y HERRAMIENTAS QUE AYUDAN A LA GESTIÓN SOBRE LA PROTECCIÓN DE DATOS.

A día de hoy existen una gran cantidad de entidades puestas a disposición de empresas y ciudadanos en cuanto a la protección de datos se refiere, por lo que clasificándolo a nivel europeo y estatal encontramos que son conocidas y de carácter obligatorio por el Reglamento: el Grupo de Trabajo (GT29), que se encuentra restructurado debido a la derogación parcial de la legislación que lo regulaba, el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD), y, por otro lado, a nivel nacional es la AEPD el organismo encargado de velar por la protección, que a su vez facilita y difunde unas herramientas de carácter gratuito.

### 8.1. El Grupo de Trabajo del Artículo 29 y el Comité Europeo de Protección de Datos.

El Grupo de Trabajo del Artículo 29 (GT29), haciéndose valer de su nombre, se trata de un órgano creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, de carácter consultivo y compuesto por un conjunto de figuras que buscan ofrecer una orientación sobre los criterios en materia de protección de datos, así como supervisar la aplicación de directrices. Fue creado en 1996 y está formado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos (SEPD) y la Comisión Europea.

Se produjeron una serie de cambios con la introducción del RGPD de manera que este quedó restructurado y actualmente el GT29 fue incluido junto al SEPD en un nuevo organismo llamado Comité Europeo de Protección de Datos (CEPD). El CEPD fue creado por el RGPD y como función principal debe aplicar correctamente el mismo. En esencia el CEPD viene a desarrollar la misma labor que ejercía el GT29, es decir, ofrecer una orientación sobre los criterios en materia de protección de datos, así como supervisar, por lo que de igual manera se trata de un organismo con personalidad jurídica propia. Para el caso concreto de España, es la AEPD la encargada de representar en el CEPD a las autoridades de protección de España.

### 8.2. Supervisor Europeo de Protección de Datos.

El Supervisor Europeo de Protección de Datos es una autoridad independiente que tiene como cometido garantizar el cumplimiento de la protección de datos en los organismos que supervisa, es decir, cumple una función de control con respecto a órganos e instituciones europeas. Concretamente el SEPD cumple tres funciones principales: supervisión, consulta en cuanto que asesora a la Comisión Europea, Parlamento Europeo y al Consejo de la Unión Europea; y de cooperación. Tiene a su disposición como apoyo al GT29 para garantizar el cumplimiento de las normas sobre protección de datos establecidas. Las competencias de esta autoridad vienen establecidas en el Reglamento (CE) nº 45/2001.

### 8.3. Las herramientas de la AEPD.

La ya citada AEPD dispone de diferentes herramientas a disposición del ciudadano de manera gratuita:

a) Facilita, la herramienta para autónomos y PYMES: Se trata de una herramienta gratuita que tiene como objetivo hacer que las empresas se adapten de manera correcta al RGPD. Será exclusivamente de uso para empresas que trabajasen con datos de escaso riesgo.
b) Gestiona EIPD: Se trata de otra herramienta de carácter gratuito orientada como asistente para usuarios a modo de guía para la

explicación de elementos básicos para el análisis de riesgos y evaluaciones de impacto en protección de datos en base a lo dispuesto en el RGPD y LOPDGDD.

c) Informa RGPD: Por último, la herramienta INFORMA_RGPD, al igual que las anteriores de carácter público y gratuito tiene como finalidad prestar soporte en aquellas dudas y cuestiones que puedan derivarse de la aplicación del RGPD.

También podemos encontrar a nivel estatal algún que otro organismo como el Centro Criptológico Nacional Computer Emergency Response Team, (CCN–CERT), creado en 2006 e integrado en el Centro Criptológico Nacional, que a su vez se encuentra adscrito como organismo al Centro Nacional de Inteligencia. De esta manera el CCN-CERT, que dispone también de herramientas a disposición, tiene como función la defensa del campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

## 9. PRINCIPIOS GENERALES DEL RGPD Y LA LOPDGDD.

Los principios generales de la LOPDGDD y del RGPD se articulan sobre la base y como necesidad para el correcto funcionamiento y protección en el tratamiento de datos personales.

Con el objetivo de comprender la importancia de los principios fundamentales en el tratamiento de datos, el Considerando 26 del RGPD establece que deben aplicarse a toda la información relativa a una persona física identificada o identificable, pero no a la información anónima, es decir, información que no haga identificable a una persona física.

### 9.1. Principio de licitud, lealtad y transparencia.

El principio de licitud se encuentra regulado en el artículo 6.1 del RGPD, junto con el de transparencia y lealtad, el cual viene a tratar el consentimiento libre e informado del interesado como pilar fundamental, pero también se regula en el mismo las excepciones al consentimiento del afectado, tales como el cumplimiento de una obligación legal o interés público. El propio RGPD especifica que el interesado tendrá derecho a solicitar y acceder a los datos personales

recogidos para verificar la licitud de los mismos. Para el caso de que el consentimiento se aplique en menores será necesario la edad mínima de 16 años, con la posibilidad y como ya se dijo anteriormente, de que cada Estado Miembro decida una inferior si lo estiman conveniente, como ocurre en España, que será a la edad de 14 años.

A diferencia de los establecido en el RGPD, en la LOPDGDD no se hace mención expresa, pero si se aprecian símiles y connotaciones que hacen alusión mediante supuestos a la licitud del tratamiento. El hecho de que no sea nombrado con carácter exclusivo en la legislación no implica ni hace exención sobre la obligación en cuanto a su cumplimiento a través de la normativa europea.

El principio de lealtad en la legislación viene regulado en el artículo 5.1. a) del RGPD, que viene a tratar la lealtad como un principio con la obligación de seguir para el correcto funcionamiento en el tratamiento de los datos personales del interesado. Este principio se encuentra vinculado con el de transparencia, de manera que los interesados deben ser plenamente conscientes de que los datos personales que requieran u otorguen tienen una validez y están ligados al funcionamiento en su tratamiento.

Al igual que ocurre en el principio de lealtad, el principio de transparencia viene regulado en el artículo 5 del RGPD, pero no es citado expresamente, aunque en el considerando 39 se expresa y delimita el contenido del mismo al nombrar la obligación de que las personas físicas serán conocedores de la recogida, uso y consulta de los datos que les concierne, así como deben existir unas medidas adecuadas que garanticen la seguridad y confidencialidad de los datos. La información se facilitará de manera verbal, escrita o por medios electrónicos.

Dicho principio se concreta en la obligación del responsable del tratamiento de datos facilitando datos personales al interesado cuando este pudiera acreditar su identidad, es decir, se pretende facilitar el derecho a obtener confirmación y comunicación a los interesados sobre los datos personales que les conciernan.

El principio de transparencia en la LOPDGDD viene regulado en el artículo 11 donde se establece que se puede llevar a cabo el cumplimiento del derecho a la información en dos capas, una primera capa con información básica y una segunda capa que contuviera el resto de la información.

9.2. Principio de compatibilidad.

El principio de compatibilidad afecta al tratamiento de datos personales con especial relevancia cuando se trata del uso y manipulación de datos con fines distintos de aquellos para los que hayan sido recogidos inicialmente, permitiendo estos cuando fueran compatibles con los fines de recogida y acudiendo a las circunstancias reguladas en el artículo 6.4 del RGDP cuando el tratamiento de datos para otro fin distinto no esté basado en el consentimiento del interesado o similares, que salvaguarde la seguridad de los datos.

De esta manera para poder afirmar si, como se ha dicho anteriormente, el tratamiento para otro fin distinto de aquel recogido inicialmente se produce o no, dependerá de la relación entre los fines distintos en los que aplicar los datos, el contexto de su recogida, la naturaleza de los datos y la existencia de unas garantías adecuadas para su protección.

Respecto a cómo dicho principio afecta a la LOPDGDD, este establece que el tratamiento de datos para la investigación en salud podrá dar lugar a la reutilización de los mismos cuando, en el caso de que hubieran sido recogidos en un primer lugar con el correspondiente consentimiento para una finalidad, se utilicen con el área que originalmente integrase el estudio inicial.

### 9.3. Principio de proporcionalidad.

El principio de proporcionalidad obliga a que los datos recabados se encuentren adecuados, pertinentes y limitados al fin para el que fueran tratados, es decir, pudiendo excepcionalmente tratar los datos personales solamente si la finalidad no pudiera lograrse razonablemente por otros medios.

El RGPD regula el principio de proporcionalidad en su artículo 5.1 c), especificando su estrecha vinculación con el principio de minimización de datos.

Ocurre lo contrario en la LOPDGDD, ya que la misma no hace referencia sobre la proporcionalidad a excepción de la remisión que realiza al Reglamento.

### 9.4. Principio de exactitud.

Con el nuevo reglamento el principio de exactitud exige que los datos sean exactos y actualizados. Por lo tanto, el responsable del tratamiento deberá actuar con la diligencia necesaria con el fin de asegurar que los datos sean correctos, completos y actuales, y es en este punto donde hace aparición el principio de exactitud, principio por el cual se determina tanto la exactitud como la actualización, permitiendo al responsable hacerlo cuando fuera necesario, ajustándose a la realidad del interesado.

Se regula en el RGPD en su artículo 5.1 d) donde se deja claro la relación de este principio con el derecho de rectificación para los casos de que no fuera correcto el tratamiento de datos. Por otra parte, en la LOPDGDD dicho principio se encuentra recogido en el artículo 4 del Título II, donde, además, se hace remisión al RGPD.

### 9.5. Principio de confidencialidad.

El principio de confidencialidad tiene como objetivo mantener resguardada la información correspondiente a los datos personales del interesado. Estipula que los datos personales otorgados por el interesado que se encuentran en disposición de un tratamiento deben estar blindados de la seguridad apropiada, ya fuera por el posible uso incorrecto, correspondiendo en dicho caso las medidas para arreglar la situación, como por el uso de ilegal de los mismos.

Este se encuentra regulado en el RGPD, en su artículo 5.1 f), donde se velará por su protección y seguridad ante un posible uso inadecuado, obligando inclusive a terceros encargados del tratamiento a la confidencialidad de los datos.

La LOPDGDD también recoge este principio y lo regula en su artículo 5, que, al igual que ocurre en el RGPD, establece su función como un deber respecto de los encargados de los tratamientos de datos en defensa de los datos personales.

## 10. LOS DERECHOS FUNDAMENTALES DE LA PROTECCIONS DE DATOS (ARCO).

Los derechos ARCO surgen de la necesidad de otorgar al ciudadano protección sobre sus datos de carácter personal. Se constituyen como un conjunto de derechos donde cada inicial del nombre representa un derecho fundamental de protección de datos para el ciudadano, hablamos de acceso, rectificación, cancelación y oposición, que en su origen se encontraban recogidos en la LOPD y que posteriormente con la llegada del RGPD fueron ampliados con la limitación y portabilidad. Son derechos cuyo ejercicio es personalísimo, es decir, que sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado.

### 10.1. Derecho de consentimiento y rectificación.

El derecho fundamental a la protección de datos se encuentra sustentado sobre dos pilares fundamentales: el consentimiento, entendido como un ejercicio de autodeterminación de la persona y el entramado conjunto de derechos que se encuentran detrás de este consentimiento que hace posible la garantía, seguridad y control de los datos.

En un primer lugar, para que el tratamiento de datos personales del interesado sea considerado lícito y obligatorio, debe realizarse conforme a derecho, y, es en este momento donde entra en juego el RGPD.

El principio del consentimiento viene regulado en el artículo 7 del RGPD, el cual indica en su extensión las diferentes capas que hacen posible el uso consensuado de los datos, donde el interesado, en una primera toma de contacto, deberá prestar consentimiento con el añadido de haberlo aportado libremente, lo que indica la comprensión de tal aceptación y si el tratamiento tuviera diferentes fines, la de ellos también.

Existirán ciertos casos en los que el consentimiento deba ser explícito, es decir, mediante una declaración escrita, por el grave riesgo o especial protección en relación con el elevado nivel de control sobre ese tipo de dato personal. Cualquier otra forma fuera de esta, hablamos de declaraciones verbales o digital, pueden conllevar dificultad en su verificación sobre el cumplimiento de las condiciones.

El RGPD viene a regular para el caso de datos personales los catalogados como especiales, como la transferencia de estos a terceros países, donde solo podrán ser objeto de tratamiento los datos si se ha otorgado consentimiento explícito del interesado.

En cuanto a cómo regula la LOPDGDD el consentimiento, este remite en casi a su totalidad a la RGPD, el cual lo regula en su artículo 6, con la excepción de datos relacionados con categorías especiales de datos, de naturaleza penal e información de carácter público.

Por parte del interesado, en todo momento ostentará la posibilidad de revocar el consentimiento otorgado, que no afectará a la licitud del tratamiento basado en el consentimiento previo a su retirada, como indica el artículo 7.

La materia del consentimiento sobre protección de datos afecta también a menores de edad, ya que se hace especial referencia a ellos por tratarse de objetivos más vulnerables, ello viene regulado en el artículo 38 del RGPD. De esta manera, y según lo dispuesto en el artículo 8.1 del RGPD, que hace referencia al tratamiento de los datos personales del menor, se pedirá un mínimo de 16 años para que se considere lícito el consentimiento del mismo. Para cualquier otro caso donde el menor tuviera una edad inferior a los 16 será necesario si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

De cualquier modo, y como ya se ha comentado anteriormente, se permite establecer por parte del Estado Miembro una edad inferior a la designada, siempre que no fuera inferior a los 13 años, por lo que España en su LOPDGDD establece la edad en 14 años.

El consentimiento de los interesados es regulado en el artículo 4.11 del RGPD, donde deja de manifiesto la necesidad de que la voluntad se considere libre e inequívoca, por lo que cualquier acto contrario a este debe ser considerado como una clara no aceptación de consentimiento. Para una correcta aplicación del consentimiento, el interesado deberá estar mínimamente informado por parte del responsable y podrá retirar su consentimiento cuando estime oportuno sin sufrir perjuicio alguno.

Por otra parte, unido al consentimiento como derecho fundamental de protección de datos se encuentra el derecho de rectificación, entendido como la facultad que se concede a personas físicas o jurídicas, regulado en el artículo 16 del RGPD. Se trata de un derecho del interesado sobre los datos personales inexactos que le conciernan, de manera que debe ponerse a disposición del interesado mecanismos que hagan posible la solicitud para la posterior rectificación, tal y como indica el artículo 65 del RGPD. De igual manera el derecho de rectificación viene regulado en el artículo 14 de la LOPDGDD, que remite al RGPD.

10.2. Derechos de los interesados y limitaciones.

Los derechos de los interesados vienen regulados en el RGPD, concretamente en su Capítulo III, dedicado a regular los Derechos de las personas. Se recogen igualmente estos derechos en el Título III de la LOPDGDD.

El derecho a la protección de datos no es un derecho fundamental absoluto, la limitación en materia de protección de datos otorgada al interesado supone un derecho por el cual, este puede solicitar al responsable del tratamiento un mayor control sobre sus datos personales. El derecho a la limitación viene regulado en los artículos 18 y Considerando 67 del RGPD. En definitiva, el RGPD impone a los responsables del tratamiento una obligación de facilitar el ejercicio de sus derechos a los interesados.

El derecho de limitación, regulado en el artículo 18 de la RGPD y 16 de la LOPDGDD, puede enfocarse desde diferentes perspectivas. En virtud de la aplicación se puede instar al responsable para que se limite el tratamiento de datos personales cuando concurriera las circunstancias específicas recogidas o bien, otra perspectiva, desde las limitaciones correspondientes al ejercicio de los derechos del interesado reflejadas en el Considerando 63 y 73 del RGPD, a través de los cuales se hace especial alusión a que los derechos y libertades del interesado se deben proteger con el límite negativo de que no afectará por ello los derechos y libertades de otras personas. Además, dicho articulado deja abierta la posibilidad de imponer restricciones a principios o derechos en la medida de lo necesario en post del interés público.

Una de las obligaciones impuestas de mayor transcendencia está relacionada con el responsable del tratamiento, que debe informar sobre los sistemas o medios a utilizar y el tratamiento a realizar, es decir, limita las posibles acciones o solicitudes por parte del interesado.

10.3. Derecho de acceso.

Es el derecho que tiene toda persona a obtener información sobre el tratamiento de sus datos personales, así como del tratamiento a los que estos se ven sometidos. Es, junto al derecho de

rectificación, uno de los derechos mencionados expresamente en el artículo 8.2 de la Carta de los Derechos Fundamentales de la Unión Europea.

El RGPD regula el contenido del derecho al acceso en el artículo 15, a través del cual se exterioriza la posibilidad de acceso por parte de los interesados a los datos personales que les conciernen, además de reconocerse al interesado el derecho a saber si se realizan tratamientos sobre sus datos. La LOPDGDD regula el derecho de acceso en su artículo 13, que remite al RGPD.

Los medios disponibles sobre el acceso a los datos personales se deberán informar por parte del responsable del tratamiento al interesado, pero para el caso de que el interesado fuera menor se realizaría a través del representante legal.

Para que el responsable del tratamiento pueda otorgar acceso al interesado sobre sus datos personales es necesario la identificación de la persona, es decir del interesado, regulado en el artículo 12 del RGPD, donde el responsable debe otorgarlo de forma accesible con un lenguaje sencillo. Por su parte, el responsable del tratamiento tiene obligación de dar respuesta a toda solicitud sobre el ejercicio de derechos en el plazo máximo de un mes desde su recepción, con posibilidad de extensión hasta los dos meses para casos excepcionales. En el caso de incumplir por parte del responsable de tratamiento el acceso del interesado se impondrán las infracciones del artículo 83 del RGPD.

### 10.4. Derecho a la supresión de los datos y derecho al olvido.

El derecho a la supresión de los datos y el derecho al olvido viene regulado en el artículo 17 del RGPD que habla sobre la importancia de que el interesado obtenga acceso a la supresión de los datos que puedan relacionarlo. La LOPDGDD lo regula en su artículo 15, que remite al RGPD, pero añade la novedosa regulación de datos referido a personas fallecidas, que será objeto de análisis más adelante como ya se indicó, otorgando a las personas vinculadas por razones familiares o de hecho al fallecido la posibilidad de solicitar el derecho de supresión de datos.

Tal y como establece el Considerando 65, los datos personales que hagan identificable al interesado se pueden suprimir a petición del mismo.

De esta manera el responsable del tratamiento debe informar al interesado de todas las posibilidades a su disposición, es decir, de la existencia del uso de esos datos personales, así como de su acceso y supresión si esta fuera pedida, habiendo de cumplir el responsable con los plazos establecidos para la supresión.

En cuanto al derecho al olvido, este se trata de la manifestación del derecho de supresión aplicado a la red, es decir, Internet. Se aplica en los casos en los que se desee eliminar información personal de Internet cuando atente contra el derecho al honor, a la intimidad o a la propia imagen, y se trata de la supresión especifica de cualquier información personal contenida en los buscadores de internet cuando no estuviera adecuada a la norma. El derecho al olvido se encuentra altamente vinculado al derecho de supresión, de manera que el derecho de supresión complemente al olvido. Otra ocasión muy común de uso de este derecho es cuando se trata de información obsoleta.

En definitiva, supone aportar al derecho de supresión una dimensión más amplia con vistas a reforzar los entornos on-line, con sus correspondientes excepciones o límites basados en interés público o en el ejercicio del derecho a libertad de expresión.

### 10.5. Derecho de oposición.

A través del derecho de oposición se permite al interesado oponerse al tratamiento de sus datos personales por parte del responsable del mismo.

El RGPD lo regula en su artículo 6.1 e) y f). Los casos recogidos y comunes sobre la oposición por parte del interesado de sus datos personales y cuando podrá solicitarla son:

a) Aquella basada en una situación particular cuando los datos personales que le conciernan sean objeto de un tratamiento.

b) Al tratamiento de datos con fines de mercadotecnia directa. En este caso la LOPDGDD especifica la validez del tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quien se hubiesen opuesto a recibirlas.

c) Al tratamiento de fines de investigación científica o históricos o con fines estadísticos.

La LOPDGDD también regula este derecho en su artículo 18, que remite a lo dispuesto en el RGPD, pero realiza un añadido para el tema de ejercitar el derecho de oposición en menores de 14 años, que serán los titulares de la patria potestad los que podrán ejercitar en su nombre y representación la oposición.

### 10.6. Derecho de transparencia e información.

Los derechos a la transparencia e información del interesado se encuentran regulados en los artículos 12, 13 y 14 del RGPD, donde se ha optado por una clasificación basado en un sistema de información por capas, que establece en primer lugar un conjunto de datos básicos y en un segundo información detallada. La LOPDGDD lo regula en el artículo 11 haciendo alusión y remitiéndose a lo dispuesto en el RGPD, con el único añadido referido a los datos y al modo de obtención de los mismos, obligando a incluir las fuentes de las que proceden los datos.

El objetivo del derecho de transparencia es reforzar el derecho de acceso a la información relativa a la protección de datos, que debe ser facilitada por escrito, verbal o medios electrónicos de manera común. La información debe ser proporcionada de manera visible, inteligible y con un lenguaje sencillo para el entendimiento del interesado, de igual manera ocurre con los plazos, otorgando entre uno a dos meses para el tiempo en el que los interesados deben recibir la información sobre el tratamiento de sus datos personales.

### 10.7. Derecho a la portabilidad de los datos.

El derecho a la portabilidad está vinculado con el derecho de acceso, la portabilidad tiene como objeto facilitar la movilidad de los datos del interesado a petición del mismo. La regulación está recogida en el artículo 20 del RGPD, que reconoce un nuevo derecho a los interesados, así como a recibir y transmitir los datos personales sin perjuicio para el interesado. Por parte del interesado, tiene como obligación respecto del responsable del tratamiento de facilitar consentimiento sobre los datos personales, es decir, se debe cumplir unos requisitos referidos y regulados en base al consentimiento por medios automatizados. Aun así, puede darse el caso de que se imponga restricciones a la portabilidad proporcionalmente al interés público.

La LOPDGDD se limita en su artículo 17 a remitirse a lo dispuesto en el RGPD, con el añadido de reconocer el derecho a portabilidad en servicios de redes sociales y servicios de la sociedad de la información equivalentes.

## 11. EL COVID-19 Y SU INFLUENCIA EN LA PROTECCIÓN DE DATOS.

La situación acontecida respecto a la pandemia, que ha afectado a nivel global, con la aparición del COVID-19, ha obligado a los estados, tanto dentro como fuera de la Unión Europea (UE), a proclamar en la mayoría el estado de alarma. Dicho estado de alarma se trata de, para el caso concreto de España, aquel recogido en el artículo 116.2 de la CE, que es de aplicación nacional. Surge ante sucesos de necesidad como grave riesgo, catástrofe o calamidad pública, situaciones de desabastecimiento de productos de primera necesidad, paralización de servicios públicos esenciales para la comunidad y crisis sanitarias, como es el caso.

Es acordado en Consejo de Ministros por un plazo no superior a 15 días, siendo imposible su prorroga sin el consentimiento del Congreso de los Diputados, que determinará el alcance y duración del mismo.

El estado de alarma viene regulado en la Ley Orgánica 4/1981 de 1 de junio, de los estados de alarma, excepción y sitio, donde son descritas medidas de carácter urgentes y extraordinario para permitir las garantías, así como las limitaciones de los ciudadanos.

Con anterioridad, España solamente había declarado el estado de alarma para la crisis de los controladores de 2010, con motivo del cierre del espacio aéreo debido a la huelga de controladores.

De esta manera se declara a través del Real Decreto 463/2020, de 14 de marzo, el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, como medida extraordinaria donde se limitaba los movimientos de los ciudadanos en todo el territorio nacional, que culminó con la vuelta la normalidad, bajo especiales restricciones, el 21 de junio, declarándose en el BOE lo siguiente: *"En base a la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio, se declaró, mediante el Real Decreto 463/2020, de 14 de marzo, el estado de alarma en todo el territorio nacional con el fin de afrontar la crisis sanitaria, el cual ha sido prorrogado en seis ocasiones, la última mediante el Real Decreto*

*555/2020, de 5 de junio, hasta las 00:00 horas del día 21 de junio de 2020, en los términos expresados en dicha norma".*

Junto con la imposición del estado de alarma surgieron por parte de ciudadanos y empresas preocupaciones en cuanto al tratamiento de datos se refiere, destacando la transparencia, por parte del Consejo de Transparencia y Buen Gobierno (CTBG), que durante la vigencia del Real Decreto y con posterior comunicación quedó paralizada, dejando con vigencia exclusivamente el acceso a la información pública, otorgando un funcionamiento básico de lo indispensable para la protección en post del interés general.

Por ello, centrándose el análisis en la situación que ha provocado el estado de alarma, cabe destacar un grupo especial de datos, que con mayor posibilidad pudieran haberse visto afectados en cuanto a la protección de datos. Desde la CCN-CERT (Centro Criptológico Nacional Computer Emergency Response Team), ya nombrada anteriormente, como organismo responsable de la ciberseguridad en España, se han realizado diversos comunicados relativos al sector del teletrabajo y a los datos personales sobre la salud:

*"Ante las circunstancias generadas por la pandemia del COVID-19, el CCN-CERT, del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia, CNI, ha reforzado todas sus capacidades para la defensa del ciberespacio español y, en especial, de su sector público y de los sectores estratégicos, con prioridad absoluta en el de la salud.*

*Su Equipo de Respuesta a Incidentes está a pleno rendimiento, brindando apoyo y colaboración a todas las organizaciones ante cualquier emergencia que puedan sufrir. Todo ello, con el firme propósito de mantener su papel como centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques, incluyendo la coordinación a nivel público estatal de los distintos CERT/CSIRT."*[1]

Además, ha sido publicado un informe debido a la situación extraordinaria, referido a la ciberseguridad del teletrabajo bajo el título de *"CCN-CERT BP/18 Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia."*

En este informe se hace especial alusión a las recomendaciones y medidas de prevención electrónicas para el correcto desempeño del empleo a través de la nube, es decir, del acceso online.

[1] https://www.ccn-cert.cni.es/cibercovid19.html

### 11.1. El teletrabajo como sustituto temporal.

Uno de los problemas y mayores inconvenientes que se han planteado en cuanto a la crisis provocada por el COVID-19, es la de recurrir a herramientas como el teletrabajo para poder seguir desempeñando las labores profesionales. Dicha situación ha hecho surgir un aumento en el temor de las empresas, relacionado con la posibilidad de sufrir ciberataques o la manipulación de información delicada y esencial fuera del entorno empresarial, que puede ocasionar la posibilidad de filtración de los datos personales protegidos.

Es por ello que la CCN-CERT y la AEPD han manifestado en diferentes informes la necesidad de extremar precauciones, pero manteniendo un ritmo de trabajo habitual al que se exigía, y que, para el caso de producirse alguna brecha o filtración en la seguridad, seguir los procedimientos que anteriormente ya estaban estipulados por los mismos, relativos a la notificación a las entidades pertinentes en un plazo de 72 horas, así como al interesado de los datos puestos en riesgo si fuera necesario. Por ello la AEPD ha emitido claramente su posición, debiendo seguir cumpliendo la normativa contemplada tanto en el LOPGDD y la RGPD, salvaguardado así el derecho fundamental a la protección de datos.

El teletrabajo, por su parte, se trata pues del resultado de algunas empresas de impedir el cese total de actividad empresarial, pero dicha excepción no implica el incumplimiento de lo ya estipulado en cuanto a protección de datos se refiere. Es una modalidad laboral que ya se encontraba recogida en el Estatuto de los Trabajadores, en el artículo 38.4. De esta manera, las empresas están obligadas a optar por diferentes políticas de medidas técnicas y organizativas de seguridad en protección de datos para garantizar la seguridad en el tratamiento de datos personales, así como hacer velar la posible entrada en conflicto de dicha situación con el derecho a la desconexión digital regulada en la LOPDGG

En definitiva, la postura por parte de las empresas de adoptar un modelo de teletrabajo no debe suponer la infracción de la normativa, ya que es de especial importancia que se siga manejando y realizando de manera ordinaria el cumplimiento de la normativa en materia de protección de datos, e incluso adquiriendo si fuera necesario una mayor relevancia por la especial situación de vulnerabilidad.

11.2. El tratamiento de datos relativos a la salud ocasionado por la pandemia.

En cuanto al análisis sobre como el estado de alarma ha afectado al tratamiento de datos personales, concretamente referido a los datos de categoría especial como son los relativos a la salud, que se encuentran citados al comienzo del artículo 9 del RGPD siendo definidos como aquellos referidos a la salud mental o física de una persona, es decir, que revelen información sobre su estado de salud, el artículo 9.1 del RGPD recoge en una simple sucesión las categorías especiales de datos que se encuentran recogidas, dejando claro la especial importancia y salvaguardia de los mencionados, que, acto seguido, en el 9.2 posibilita su cancelación en cuanto a dicha protección, para el caso de que concurriera como explica en su apartado i): razones de interés público en el ámbito de la salud pública y la protección de la asistencia sanitaria que será el objeto a analizar. De esta manera, se permite el tratamiento de esos datos, pero siempre sujeto a esa condición de especial gravedad, que determinarán las autoridades sanitarias.

En cuanto a la LOPDGDD, este en su artículo 6 se limita a hacer referencia a lo estipulado en el RGPD, permitiéndose la licitud del tratamiento de datos personales para la investigación de la salud, cuando se trate de situaciones de excepcional relevancia y gravedad para la salud pública.

La AEPD se ha pronunciado sobre el tema, alegando que, frente a una situación de crisis, se hace necesario ciertas restricciones a la privacidad de datos, que como se ha observado, ya se encontraban recogidas en nuestra legislación, haciendo prevalecer las razones de interés público, aludiendo en este caso al tratamiento de datos personales regulado en el artículo 6.1. e) del RGPD, donde se legitima por motivos de interés público la licitud de estos.

Todo lo dispuesto viene reconocido por la AEPD en su informe N/REF: 0017/2020, donde da respuesta a la legitimación del tratamiento de datos de salud en relación con el COVID-19.

Por su parte, el CEPD, que se define en su página web como, "*El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE*"[2], emitió, al igual que la AEPD, una serie de informes que inciden en la idea por la cual las normas de

[2] https://edpb.europa.eu/about-edpb/about-edpb_es

protección de datos no deben obstaculizar las medidas adoptadas por la pandemia del coronavirus, siempre que estas sean necesarias, apropiadas y proporcionadas.

La incertidumbre sobre cómo proceder ha dado lugar a múltiples situaciones, que ha despertado especial interés en cuanto al tratamiento de los datos de salud y por ello mediante el FAQ sobre el COVID-19, la AEPD ha tratado de dar respuesta a las preguntas relativas al tratamiento de datos:

1) Una de ellas ha sido el de la toma de temperatura previa como indicador y posible requisito en ciertos establecimientos, lugares o empresas para evitar minimizar en lo posible el contagio. En un primer lugar, es la misma AEPD, en virtud del RGPD, el que reconoce la posibilidad de efectuar un protocolo bajo los estándares de unas correctas garantías adecuadas, exigiendo el uso exclusivo de finalidad de los datos recogidos para detectar posibles personas contagiadas y que dicho control sea realizado por personal sanitario o en cuyo caso personal de seguridad.

2) Por otra parte, a través de la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19, que solicita medidas en relación con la geolocalización de los usuarios es que surge, por parte de diferentes comunidades autónomas, herramientas tecnológicas en formato web, así como versiones APP en IOS y Android, que permiten realizar una autoevaluación del estado de salud de los ciudadanos en función de sus síntomas, facilitando instrucciones y recomendaciones sobre el COVID-19. De esta manera se pretende ayudar a evitar el actual colapso del sistema sanitario. Uno de los ejemplos más cercanos ha sido el caso de Andalucía, en su APP móvil Salud Responde, que ha habilitado un asistente virtual y la posibilidad de geolocalización con la idea de saber más sobre el virus y paliar su propagación. Entre los datos que la APP recoge, como nombre, número de teléfono móvil, DNI/NIE, etc., el que mayor preocupación ha generado es el relativo a la geolocalización debido a que conlleva un sistema de recogida de datos categorizados como de especial protección ante los que pudiera dar lugar a una brecha de seguridad, puesto que se tramitan los datos a través de un formato web, que se almacenan en bases de datos de organismos de salud.

El sistema de geolocalización fue acordado como completamente voluntario para el usuario y consistió en un análisis del movimiento realizado durante la duración del estado de alarma, que posteriormente era enviado a través de las operadoras móviles al Instituto Nacional de Estadística.

## 12. PROTECCIÓN DE DATOS Y PREVENCIÓN DE DELITOS, ESPECIAL RELEVANCIA AL RÉGIMEN JURÍDICO ESPAÑOL SOBRE ÁMBITO PENAL.

Todo lo anterior dispuesto deja claro que, aunque se pueda ocasionar brechas en la seguridad debido a la situación o restringir derechos en base al interés público, tanto la AEPD, en España, junto con la correspondiente regulación vigente, así como diferentes órganos de la UE, que buscan la minimización del daño en cuanto a la protección de datos, han dejado clara su postura en cuanto al requisito de salvaguardia del mismo, llegando a sancionar al que incumpliera lo dispuesto en la ley.

Aplicable a la infracción de cualquier derecho recogido relativo a la protección de datos, el artículo 83 del RGPD, bajo el nombre de "Condiciones generales para la imposición de multas administrativas" viene a regular las sanciones que pueden imponerse por el incumplimiento del tratamiento de datos y la infracción al desempeño de dichos derechos, es decir, la difusión de datos especialmente sensibles de una persona física.

En España la competencia para investigar este tipo de actuaciones es de la AEPD y si se determina que se ha infringido el RGPD o la LOPDGDD, podrá incoar el correspondiente procedimiento sancionador contra quienes han manipulado los datos. La LOPDGDD recoge un listado de conductas que se consideran constitutivas de infracciones del RGPD, dividiéndolas en tres categorías: leves, graves y muy graves, tipificando las infracciones.

De esta manera las infracciones pueden ser sancionables con multas que puede alcanzar según el RGPD los 20 millones de euros o, para el caso de empresas, el 4% del volumen de negocio total anual global del ejercicio financiero anterior.

En la actualidad jurídica ocurre que en múltiples ocasiones se dan casos de delitos que implican un perjuicio sobre la figura de la protección de datos, es por ello que, por parte de la AEPD, se ha puesto a disposición del ciudadano medio una Guía sobre Protección de Datos y

Prevención de Delitos con un catálogo de medidas para evitar la comisión de estos delitos y para prevenir ser víctima.

En dicha guía se propone prevenir delitos relacionados con el ámbito de revelación de secretos y de carácter informático, por lo cual, se aconseja tanto el aprendizaje como el uso responsable de internet, se hace especial énfasis en los correos electrónicos y las redes sociales como espacio social. Para ello recomienda que se garantice el derecho a la educación digital prevista en el art. 83 LOPDDD, concretamente la inserción del alumnado en la sociedad digital, así como su uso responsable y respetuoso, incluyendo el ámbito de protección de datos.

Con el mismo ámbito a manejar, pero haciendo especial hincapié en la protección de datos en el proceso penal, cabe destacar el Protocolo de Comunicación de la Justicia 2018 elaborado por la Oficina de Comunicación del CGPJ, por el cual se insta a comunicar o recibir libremente información veraz referida a la especial protección de datos que supone la información judicial. El derecho a la información a la vez que constituye un derecho subjetivo de libertad cumple una función de garantías en las sociedades democráticas, que viene establecido y regulado en el art. 20 CE. De esta manera, el Protocolo elabora un mecanismo alrededor de las funciones y el obligado cumplimiento de los órganos judiciales en cuanto a los datos personales se refiere, otorgando o restringiendo acceso a estos, para evitar que los datos de las sentencias sean usados con fines contrarios a las leyes.

Respecto al régimen jurídico del derecho a la protección de datos en el proceso penal, cabe destacar que, durante los procesos penales, ocurre una circulación de datos personales necesarios para los procesos, sobre los sujetos que están siendo investigados por posibles ilícitos penales. Con esto en mente cabe destacar que para el régimen jurídico del tratamiento de los datos personales en el proceso penal no se aplica directamente el régimen normativo general (RGPD y LOPDGDD), sino la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, haciendo que la LOPDGDD y el RGPD pasen a ser de aplicación supletoria, tal como indica el art. 2.2 d) RGPD y 2.3 LOPDGDD.

Esto no quiere decir que el RGPD no contenga un régimen aplicable al tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad, puesto que viene

regulado en su artículo 10, donde determina, que el tratamiento de estos datos se podrá realizar bajo supervisión de autoridad pública o derecho de la UE o estados miembros, que garanticen derechos y libertades del interesado.

La Directiva 2016/680 se aplica de manera semejante a lo estipulado por el artículo 4 del RGPD en cuanto a la regulación del contenido de protección en lo que respecta a tratamientos de los datos y su circulación, puesto que su contenido es de por si similar, centrándose en el carácter del tratamiento de licitud, adecuación, reconoce los derechos de acceso, rectificación o supresión y limitación del tratamiento, todo ello con independencia de que en algunos de sus preceptos se disponga un carácter propio en base a su regulación.

Un detalle relevante a tener en cuenta es que la Directiva, establecía un plazo de transposición que finalizó, de tal manera que, hasta la trasposición futura de la misma, la actuación de los funciones y autoridades policiales y judiciales en el ejercicio de sus funciones seguirá regulándose por la normativa vigente interna española.

### 12.1 Tratamiento de datos en ámbito penal europeo para la protección de datos en la Orden Europea de Investigación.

La Directiva 2014/41, del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, que regula la Orden Europea de Investigación, entendida como una resolución judicial de una autoridad judicial de un Estado miembro que avala la posibilidad de llevar a cabo medidas de investigación en otro Estado miembro en beneficio de un proceso penal,  establece, en su artículo 20 que, los Estados miembros velarán por la protección de los datos personales y que el tratamiento de datos de los mismo solo puedan realizarse de acuerdo con la Directiva 2016/680, con la única limitación para el ámbito de acceso de dichos datos a las personas autorizadas que vengan establecidas en la Directiva, como ya fueron citadas anteriormente, y con arreglo a los principios del Convenio 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 y su Protocolo adicional.

En cuanto a la regulación de transferencia de datos personales a terceros países u organizaciones internacionales, viene regulado en la Directiva 2016/680.

Para el caso de que los datos personales se transfieran fuera de la UE, la organización, organismo o empresa que hubiera exportado los datos personales, debe garantizar que se cumplirán unas condiciones de salvaguardia de las mismas.

A su vez, la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, regula la posibilidad de uso en España de los datos personales conseguidos por Orden Europea de Investigación en Estado Miembro, siempre y cuando estuviera permitido, y se informara de la finalidad del uso cuando fuera necesario.

## 13. REGULACIÓN SOBRE DATOS DE PERSONAS FALLECIDAS EN LA LOPDGDD Y EN EL RGPD.

La epidemia de COVID-19 en España ha provocado un número de fallecidos a cuyos familiares se les ha denegado la posibilidad de acompañamiento o despedida de la persona difunta como medida para la seguridad de la salud pública debido al nivel de crisis sanitaria, pero ¿a qué nivel afecta esto a la legislación sobre los datos personales del fallecido en la LOPDGDD y la RGPD? Como ya se expuso anteriormente, España ha sido pionera en adaptar el texto legislativo europeo e innovar sobre los derechos de las personas ya fallecidas a través de la LOPDGDD, ya que en el Reglamento no había regulación alguna sobre los datos personales de las personas fallecidas, queriendo hacer alusión a que cada Estado miembro tuviera la oportunidad de establecer su propia regulación al respecto.

De esta manera, a través de la LOPDGDD en su artículo 3 permite que las personas vinculadas por razones familiares o, de hecho, puedan solicitar acceso, rectificación, así como la supresión de los datos personales que refieran o identifiquen a la persona fallecida. Esto no implica que la persona fallecida deje de poseer control sobre los derechos y esfera de datos personales que le rodean, puesto que la ley le otorga la posibilidad de prohibir la manipulación, con algunas excepciones, y de designar a terceros para que fueran los únicos con posibilidad de acceder a los datos a petición del fallecido.

El artículo continua su extensión, regulando los datos personales del fallecido cuando este fuera menor de edad o persona con discapacidad, delegando las facultades a sus representantes legales, por quien hubiese sido designado en el ejercicio de sus funciones, o, si fuera necesario, por el Ministerio Fiscal, que podrán actuar de oficio o a instancia.

Para el caso de no encontrar ninguna prohibición o delegación exclusiva, cualquiera de los nombrados podrá dirigirse al responsable del tratamiento de datos con la premisa de solicitar el acceso a los mismas para la rectificación o supresión.

En los últimos años este artículo y este tipo de prácticas han ido tomando especial importancia para eliminar rastros referentes a los prestadores de servicios de la sociedad de la información con regulación en la Ley 34/2002, para la eliminación de perfiles personales de redes sociales o equivalentes.

## 14. CONCLUIONES.

Con la elaboración de este trabajo se ha hecho presente la evolución histórica de la protección de datos y de cómo se ha ido formando un cambio drástico en la organización de la misma, así como de la capacidad de adaptarse a la necesidad de las nuevas tecnologías, que suponían un reto que nunca antes había ocurrido. De esta manera, y llegando a nuestros días, se plasma la idea de una legislación europea básica, necesaria y de obligatorio añadido, que todos los países miembros deben cumplir, con independencia de que posteriormente realicen un texto propio que llegue a complementar y adaptar con relativo albedrio la norma europea, como sucede en el caso de España, donde además, se les da a las figuras ya creadas hasta la fecha, con referencia a la AEPD y derivados, la administración sobre su cumplimiento y poder de sanción para el caso de que no suceda.

Por otra parte, como ya se ha dejado caer, se crean múltiples figuras totalmente necesarias, tanto a nivel europeo como de los estados miembros, que tienen como función la correcta aplicación de las normas relativas a la protección de datos y de otorgar el soporte necesario a los ciudadanos que tengan la necesidad de conocer de primera mano el funcionamiento de estas para su posterior aplicación y uso.

En cuanto a los principios generales de la LOPDGDD y del RGPD, se articulan sobre la base y como necesidad para el correcto funcionamiento y protección en el tratamiento de datos personales, que vienen a regular las propias libertades que otorgan los textos respecto a la protección de datos, pero a su vez funcionan con la doble función de limite normativo, donde en la mayoría de los casos lo que viene a realizar la LOPDGDD es una mera mención, seguida de la correspondiente alusión al RGPD. La máxima de estos principios generales gira en torno a la figura del ciudadano y como cualquier situación que pueda afectar y poner en riesgo sus

datos personales se encuentran protegidos y regulados cuando se trata del uso y manipulación de los mismos.

Volviendo al tema relativo a las nuevas tecnologías, la llegada del RGPD y su posterior adaptación con la LOPDGDD, la cual cuenta con el añadido relativo a las garantías digitales y el desarrollo de las mismas en torno al tratamiento y análisis de los datos procedentes de la Red, supuso en España el puesto como primer estado miembro en complementar el texto europeo con añadidos como la incorporación de los derechos digitales, el nuevo régimen jurídico de los empleados basados en los mismos y la gestión de datos personales de las personas fallecidas. Esto ha llevado a un nuevo marco legislativo que implica a la LOPDGDD, el RGPD y la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), que introduce matices relacionado con la prestación de servicios, dando lugar a una estrecha vinculación de esta con las dos anteriores.

También, en este documento se han recogido las razones de como los derechos ARCO constituyen parte de la legislación sobre la protección de datos a nivel estatal y tienen el objetivo de proteger los datos personales, resultando en un permiso a cualquier persona física que tuviera interés en la información que la identificase, posibilitando realizar un control sobre ella.

Además, los derechos ARCO, se encuentran actualizados a través del RGPD, el cual refuerza con el añadido de otros nuevos y modifica el procedimiento para ejercitar su protección. Estos, al igual que ha ocurrido con la legislación en torno a la protección de datos, han ido evolucionando y adaptándose a lo que son hoy día, permitiendo al ciudadano ser ejercidos a través de la figura de la AEPD en el momento en que dicha persona sintiera que de alguna manera no estaba siendo ejercida de manera correcta el tratamiento o la protección de los mismos.

Por otra parte, con la llegada del COVID-19 a nuestras fronteras y consecuentemente la promulgación del estado de alarma ha supuesto un auténtico desafío para la correcta aplicación de la protección de datos, así como para las figuras que en España eran encargadas de su cumplimiento. De esta manera, los modelos empleados por las empresas, en post del teletrabajo, hicieron surgir un añadido de especial cuidado y protección frente a la situación de vulnerabilidad en la que se encontraban, buscando el cumplimiento de la normativa en el ámbito laboral y minimización del daño, sancionando al que incumpliera lo dispuesto en la ley.

En cuanto a los datos de especial protección como son los relativos a la salud, el obligado cumplimiento del estado de alarma, en cuanto a crisis sanitaria se refiere, ha dado lugar a la

flexibilidad en ciertos casos de hacer prevalecer el interés social respecto de la protección de datos del individuo como carácter personal, permitiendo el tratamiento, que determinarían las autoridades sanitarias a través de informes, haciendo velar la protección de datos siempre y cuando no fuera necesario lo contrario.

En definitiva, una vez analizado la configuración que corresponde a la estructura alrededor de la protección de datos, cabe destacar que se encuentra actualizada y es de aplicación tanto a nivel europeo como estatal, realizándose un correcto funcionamiento de la misma en cuanto a nivel de normativa se refiere, llegando a sobresalir la validez e importancia de la misma en una eventualidad como la que ha acontecido, prevaleciendo los sistemas que ya contemplaban tal situación y que habían sido creados para paliar cualquier tipo de excepcionalidad.

## 15. BIBLIOGRAFÍA.


- AEPD, *Guía AEPD «Protección de datos y prevención de delitos»*. Recuperado 19 de febrero de 2020, de aepd website: https://www.aepd.es/media/guias/guia-proteccion-datos-y-prevencion-de-delitos.pdf
- AEPD, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*. Recuperado 20 de febrero de 2020, de aepd website: https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf
- AEPD, FAQ sobre el COVID-19. Recuperado 19 de mayo de 2020, de aepd website: https://www.aepd.es/sites/default/files/2020-03/FAQ-COVID_19.pdf
- AEPD, *GUÍA PARA EL CUMPLIMIENTO DEL DEBER DE INFORMAR*. Recuperado 25 de febrero de 2020, de aepd website: https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf
- Alarcón, V. (2018) *GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?*. Recuperado 21 de febrero de 2020, de Signaturit website: https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos
- Alina Nastasache, (2020) *La tecnología en la crisis sanitaria del coronavirus: ¿Cómo se realiza el tratamiento de los datos personales?*. Recuperado 15 de mayo de 2020, de DPO&itlaw website: http://www.dpoitlaw.com/la-tecnologia-en-la-crisis-sanitaria-del-coronavirus-como-se-realiza-el tratamiento-de-los-datos-personales/
- Asesor Digital, (2020) *Recomendaciones de Protección de Datos para teletrabajar durante el Covid-19*. Recuperado 14 de mayo de 2020, de Laver Legal Advisory and Consultancy Services website: https://www.laverconsultores.com/recomendaciones-de-proteccion-de-datos-para-teletrabajar-durante-el-covid-19/
- Asesor RGPD, (2020) *Teletrabajo y Covid-19*. Recuperado 14 de mayo de 2020, de AdaptaRGPD website: https://www.adaptacion-rgpd.eu/teletrabajo-y-covid-19/
- Ayuda Ley Protecciónd atos, *Guía adaptación de la LOPD a LOPDGDD en 2020*. Recuperado 24 de febrero de 2020, de Ayuda Ley Protecciónd atos website: https://ayudaleyprotecciondatos.es/lopdgdd/
- Ayuda Ley Protecciónd atos, *Informe AEPD sobre legitimación para el tratamiento de datos de salud*. Recuperado 12 de mayo de 2020, de Ayuda Ley Protecciónd atos website: https://ayudaleyprotecciondatos.es/2019/02/21/informe-aepd-tratamiento-datos-salud/
- Ayuda Ley Protecciónd atos, *Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)*. Recuperado 30 de abril de 2020, de Ayuda Ley Protecciónd atos website: https://ayudaleyprotecciondatos.es/2016/06/18/los-derechos-arco-acceso-rectificacion-cancelacion-y-oposicion/
- *Breve historia de la Protección de Datos Personales*. Recuperado 23 de febrero de 2020, de Oposiciones TIC website: https://oposicionestic.blogspot.com/2017/12/breve-historia-de-la-proteccion-de.html
- Carolina López Medina, EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PENAL

- Centro Criptológico Nacional, (2020) Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia. Recuperado 15 de mayo de 2020, de CCN-CERT website: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html
- Confianza Online, (2019) #TipsLOPDGDD. ¿Cuáles son los Principios en la Protección de Datos?. Recuperado 01 de marzo de 2020, de Confianza Online website: https://www.confianzaonline.es/conocenos/comunicacion/utlimas-noticias/tipslopdgdd-cuales-son-los-principios-en-la-proteccion-de-datos/
- Diario Jurídico, (2012) XX Aniversario de la LORTAD: 20 años de protección de datos. Recuperado 06 de marzo de 2020, de Diario Jurídico website: https://www.diariojuridico.com/xx-aniversario-de-la-lortad-20-anos-de-proteccion-de-datos/
- DPO&itlaw, *RGPD – Unidad III : Accountability o Principio de Responsabilidad* Proactiva. Recuperado 01 de mayo de 2020, de DPO&itlaw website: http://www.dpoitlaw.com/reglamento-general-de-proteccion-de-datos-rgpd/unidad-iii-accountability-o-principio-de-responsabilidad-proactiva/
- europa.eu, (2004) *Supervisor Europeo de Protección de Datos (SEPD)*. Recuperado 01 de marzo de 2020, de europa.eu website: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_es
- europa.eu, (2020) *Reglamento general de protección de datos*. Recuperado 17 de abril de 2020, de europa.eu website: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm#shortcut-6
- GDPR Legal, (2020) *COVID-19: Controles de temperatura y su encaje en la normativa de protección de datos*. Recuperado 23 de mayo de 2020, de AEC website: https://dpd.aec.es/covid-19-controles-de-temperatura-y-su-encaje-en-la-normativa-de-proteccion-de-datos/
- Grupo DatCon, *LOPDGDD 3/2018: Nueva Ley Orgánica de Protección de Datos y de Garantías de los Derechos Digitales*. Recuperado 21 de febrero de 2020, de GrupoDatCon-Norte website: https://grupodatcon-norte.com/ley-organica-de-proteccion-de-datos-y-de-garantias-de-los-derechos-digitales/
- Iberley, (2018) *Publicada la nueva Ley de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).* Recuperado 21 de febrero de 2020, de Iberley website: https://www.iberley.es/noticias/publicada-nueva-ley-proteccion-datos-personales-lopdgdd-29303
- Joaquín Delgado Martín, (2019) *La protección de datos personales en el proceso penal: Directiva 2016/680*. Recuperado 13 de marzo de 2020, de LEFEBVRE website: https://elderecho.com/la-proteccion-datos-personales-proceso-penal-directiva-2016-680
- Joaquín Delgado Martín, (2019) *Protección de datos personales en el proceso penal (II)*. Recuperado 13 de marzo de 2020, de LEFEBVRE website: https://elderecho.com/proteccion-datos-personales-proceso-penal-ii
- José Luis Piñar Mañas, (2020) *La protección de datos durante la crisis del coronavirus*. Recuperado 13 de mayo de 2020, de Abogacía Española Consejo General website: https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/

- Maniacs, *Niveles de seguridad en la LOPD*. Recuperado 27 de febrero de 2020, de Maniacs website: https://www.lopdencastellon.com/niveles-de-seguridad-en-la-lopd/
- Metricson, *Responsabilidad proactiva: el eje vertebrador del RGPD*. Recuperado 20 de abril de 2020, de Metricson website: https://metricson.com/2018/05/04/responsabilidad-proactiva-el-eje-vertebrador-del-rgpd/
- Nieves Chaveli Donet, (2017) *DERECHOS DEL INTERESADO EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS*. Recuperado 29 de abril de 2020, de Legal Advisor – Govertis website: https://www.govertis.com/derechos-del-interesado-en-el-reglamento-general-de-proteccion-de-datos
- *¿Qué es la LOPDGDD y cómo se aplica? Consecuencias del nuevo marco legal.* (2020). Recuperado 19 de febrero de 2020, de Cookiebot website: https://www.cookiebot.com/es/lopdgdd/?gclid=CjwKCAiA66_xBRBhEiwAhrMuLdKVpzDpTY-JrXp4wJryt-SZ6-rPZiUMDY2uvAXBVDxN7cyy7hbIxRoCIi4QAvD_BwE
- Prevent Security Systems, *RGPD y videovigilancia: ¿En qué consiste el principio de responsabilidad proactiva?*. Recuperado 01 de mayo de 2020, de Prevent Security Systems website: https://www.prevent.es/en-que-consiste-el-principio-de-responsabilidad-proactiva-en-el-rgpd
- Segundo Pérez, (2019) *EL PRINCIPIO DE TRANSPARENCIA EN LA PROTECCIÓN DE DATOS PERSONALES*. Recuperado 30 de abril de 2020, de Melián Abogados website: https://mymabogados.com/el-principio-de-transparencia-en-la-proteccion-de-datos-personales
- Super Contable, Consentimiento (Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal). Recuperado 24 de febrero de 2020, de Super Contable website: https://www.supercontable.com/informacion/ley_gestion/Consentimiento._Ley_15-1999._Proteccion_de_datos.html
- viewnext, (2019) *Artículo 17 del RGPD: derecho de supresión y olvido*. Recuperado 29 de abril de 2020, de viewnext website: https://www.viewnext.com/articulo-17-del-rgpd-derecho-de-supresion-y-olvido/
- Wolters Kluwer, *Comité Europeo de Protección de Datos*. Recuperado 01 de marzo de 2020, de Wolters Kluwer website: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwMjQ7Wy1KLizPw8WyMDQwsDU0MTkEBmWqVLfnJIZUGqbVpiTnEqAOnxMfI1AAAAWKE
- Wolters Kluwer, *Derecho a la limitación del tratamiento de datos*. Recuperado 29 de abril de 2020, de Wolters Kluwer website: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwMjY7Wy1KLizPw8WyMDQwsDU0MTkEBmWqVLfnJIZUGqbVpiTnEqAGwMUTI1AAAAWKE
- Wolters Kluwer, *Derecho de oposición (Protección de Datos)*. Recuperado 30 de abril de 2020, de Wolters Kluwer website: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwNLS7Wy1KLizPw8WyMDQwsDU0MzkEBmWqVLfnJIZUGqbVpiTnEqAHJB1Gs1AAAAWKE