FACULTAD DE DERECHO

ANÁLISIS DE LA FRONTERA ENTRE LA DEFENSA POR PARTE DE LA JURISDICCIÓN CIVIL DEL DERECHO AL HONOR, INTIMIDAD Y PROPIA IMAGEN Y LA ACTIVIDAD DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EN MATERIA DE PROTECCIÓN DE DATOS

Autor: Laura Mateos Rojas

5º E-3 B

Área de Derecho Civil

Tutor: Joaquín Ruiz Echauri

Madrid

Abril 2023

RESUMEN

¿Está perdiendo competencia el Derecho civil en favor de una expansión de la vía administrativa en lo referente a la protección de datos? Históricamente, el derecho al honor, intimidad y propia imagen, recogidos en el mismo precepto de la Constitución española que el derecho a la protección de datos, ha venido regulado por la vía civil. Sin embargo, en la nueva realidad, a raíz de la normativa europea de protección de datos y la creación de las autoridades de control independientes, se encuentran estas resoluciones de órganos administrativos -en el caso de España, de la Agencia Española de Protección de Datos- que resuelven sobre asuntos referidos a derechos fundamentales. En consecuencia, lo que inicialmente se concebía como una defensa de la cual era titular el individuo a través de la jurisdicción civil, se expande a una cuya iniciativa también recae sobre la Agencia Española de Protección de Datos.

El presente Trabajo, por tanto, pretende abordar cuál es la concreción de los límites de la protección de datos y la defensa del derecho al honor, intimidad y propia imagen por parte de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

PALABRAS CLAVE

protección de datos, AEPD, tutela civil, derecho al honor, derecho a la intimidad, derecho a la propia imagen

ABSTRACT

Is civil law losing its competence in favor of an expansion of the administrative route with regard to data protection? Historically, the right to honor, privacy and self-image, included in the same precept of the Spanish Constitution as the right to data protection, has been regulated by civil law. However, in the new reality, as a result of European data protection regulations and the creation of independent supervisory authorities, we find these resolutions of administrative bodies - in the case of Spain, the Spanish Data Protection Agency - which rule on matters referring to fundamental rights. Consequently, what was initially conceived as a defense of which the individual was the holder through the civil jurisdiction, expands to one whose initiative also falls on the Spanish Data Protection Agency.

This paper, therefore, aims to address what is the specification of the limits of data protection and the defense of the right to honor, privacy and self-image by the Spanish Organic Law 1/1982, of May 5th, on the civil protection of the right to honor, personal and family privacy and self-image and the Spanish Organic Law 3/2018, of December 5th, on the Protection of Personal Data and guarantee of digital rights.

KEY WORDS

data protection, Spanish Data Protection Agency, civil protection, right to honor, right to privacy, right to privacy, right to self-image

ÍNDICE

LISTADO DE ABREVIATURAS

AEPD – Agencia Española de Protección de Datos

CC – Código Civil

CDFUE – Carta de Derechos Fundamentales de la Unión Europea

CE – Constitución Española

CEDH – Convenio Europeo de Derechos Humanos

CEPD – Comité Europeo de Protección de Datos

DHIPI – Derecho al Honor, Intimidad Personal y Familiar y Propia Imagen

LEC – Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil

LOPDGDD – Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LOPH – Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, la Intimidad Personal y Familiar y a la Propia Imagen

LOPJ – Ley Orgánica 6/1985, de 1 julio, del Poder Judicial

RAE – Real Academia Española

RGPD – 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.

STC – Sentencia del Tribunal Constitucional

STEDH – Sentencia del Tribunal Europeo de Derechos Humanos

STS – Sentencia del Tribunal Supremo

TEDH – Tribunal Europeo de Derechos Humanos

TFUE – Tratado de Funcionamiento de la Unión Europea

TUE – Tratado de la Unión Europea

1. INTRODUCCIÓN.

1.1. Planteamiento y justificación de la cuestión.

El avance tecnológico y la llegada de la llamada Era digital supuso la necesidad de adecuar los ordenamientos jurídicos a la nueva realidad a la que se enfrentaban las sociedades actuales. Con motivo de ello, afloró una diversa producción normativa dirigida a proteger y a garantizar las distintas facetas de esta realidad, entre ellas, la protección de los datos personales de los ciudadanos con motivo del tratamiento de cantidades ingentes de datos y las posibles intromisiones en la vida privada de las personas debido a ello.

Así, el derecho a la protección de datos, también denominado derecho a la autodeterminación informativa, se configura como un derecho fundamental autónomo el cual "complementa la vertiente negativa del derecho a la intimidad" (Megías Quirós, 2019, p.146) por el cual se permite reservar del conocimiento de terceros los datos personales.

Este derecho guarda una estrecha relación con los derechos al honor, intimidad y propia imagen puesto que se encuentran recogidos en el mismo precepto constitucional, el artículo 18 CE. Por ello, como ocurre en multitud de ocasiones también con otros derechos fundamentales, la lesión del derecho al honor, intimidad y propia imagen puede suponer al mismo tiempo una lesión al derecho fundamental a la protección de datos.

En este sentido, el surgimiento de una autoridad de control independiente al mando de la defensa del derecho fundamental a la protección de datos nos plantea cuestiones como la que concierne el presente Trabajo: ¿cuál es la frontera entre la actividad de este ente y la de los tribunales civiles en la defensa de estos derechos fundamentales que en tan numerosas ocasiones se lesionan simultáneamente?

1.2. Objetivos de la investigación.

El objetivo principal de este trabajo es el estudio de los límites del artículo 18 CE en la sociedad de la información. Se estudiará cuál es la concreción de los límites de la protección de datos y la defensa del derecho al honor, intimidad y propia imagen. (en adelante, DHIPI) por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Concretamente, será objeto de análisis la frontera entre la defensa del DHIPI por parte de los tribunales

civiles y la actividad de la Agencia Española de Protección de Datos (en adelante, AEPD) y salvaguarda del derecho fundamental a la protección de datos.

1.3. Metodología y estructura de la investigación.

El presente trabajo de investigación se ha dividido en cinco capítulos distintos. En primer lugar, en el apartado segundo, se ha procedido a establecer el marco conceptual en base al cual se desenvuelve la investigación, para así asentar los elementos principales de este trabajo. En esta contextualización se ha proporcionado el hilo histórico de los derechos al honor, intimidad y propia imagen. Posteriormente, se define y explica de forma individualizada, en apartados independientes, los conceptos de honor, intimidad y propia imagen. Asimismo, se expone qué se entiende por dato como objeto de protección.

En segundo término, en el apartado tercero, el trabajo se adentra en regulación del derecho al honor, intimidad y propia imagen en el ámbito europeo, Constitucional y en el de la Ley Orgánica que desarrolla y concreta estos derechos. Con estructura equivalente, el cuarto apartado desarrolla el derecho fundamental a la protección de datos como derecho independiente y autónomo a los expuestos en el apartado precedente; asimismo, en este apartado relativo a la protección de datos, se exponen los principales derechos de los ciudadanos europeos en esta materia. El principal propósito de estos dos apartados es exponer el marco jurídico-teórico sobre el que se desenvuelven estos derechos de cara a presentar las distinciones entre ellos, así como la relación y cercanía existente entre todos ellos.

A continuación, en el apartado quinto se expone la entidad responsable de la defensa del derecho fundamental a la protección de datos, la AEPD, para detallar su actividad y competencia en esta materia. Al respecto, se ha expuesto la configuración de la entidad, así como sus funciones.

Por último, en el apartado sexto se desarrolla la problemática objeto de esta investigación de cara a estudiar la presencia, o no, de una actividad expansiva de la AEPD, frente a la actividad de la jurisdicción civil en materia de protección del DHIPI. Para ello se estudiarán las materias de las que se declara competente la AEPD y aquellas que rechaza, así como los motivos de ello, de forma similar a la actividad de la jurisdicción civil.

Metodológicamente, esta investigación se ha nutrido de diversas fuentes, tanto doctrinales como jurisprudenciales. Se ha acudido a artículos y revistas jurídicas, trabajos de otros

autores, así como a la legislación y jurisprudencia con el fin de realizar una investigación íntegra.

2. MARCO CONCEPTUAL.

2.1. Contexto histórico. Origen del derecho al honor, intimidad y propia imagen.

El DHIPI pertenece a la categoría de los derechos de la personalidad, actualmente tiene rango de derecho fundamental en la Constitución Española, estando recogido en su artículo 18.1. Este tipo de derechos "protegen bienes inherentes a la personalidad humana" (cfr. Rodríguez Guitián, 1995).

Sin embargo, a pesar de su actual posición en nuestro ordenamiento jurídico, los derechos de la personalidad no siempre han sido reconocidos y protegidos. El reconocimiento de estos derechos en los distintos ordenamientos jurídicos no es un evento temporal ni territorialmente homogéneo (Rogel Vide, 2007).

En este sentido, los derechos de la personalidad entendidos como tal empiezan a surgir a lo largo de la segunda mitad del siglo XIX. No obstante, esto no implica que el objeto de esta protección, estos bienes, no estuviesen salvaguardados con anterioridad: en Derecho romano existía la figura de la *actio iniuriarum* para la persecución de la injuria, entendida como aquel acto que lesiona, física o moralmente, a la propia persona (*Ibid*.).

En esta misma línea, en Grecia, de forma similar, existía la *dike kakegorias* que, de forma similar a la acción de Derecho romano, esta también castigaba las ofensas físicas y morales (Rodríguez Guitián, 1995).

A pesar de estos inicios, el avance de los derechos de la personalidad y su protección no vio la luz en las sociedades modernas hasta que los ciudadanos consiguieron una seguridad mínima frente al poder estatal para poder entonces trasladar sus inquietudes al ámbito privado (Rogel Vide, 2007). Así, dado que el escenario social había cambiado, el hombre comenzó a ver necesaria la defensa frente a las ofensas procedentes de otros particulares (Rodríguez Guitián, 1995).

En cualquier caso, para reconocimiento completo de estos derechos, sería necesario el reconocimiento de la igualdad de todas las personas. Sin embargo, las prácticas realizadas en la Antigua Roma relativas a considerar a los esclavos como cosas susceptibles de tráfico jurídico incluso desde su gestación -a modo de compraventa de cosa futura-, no se alejan tanto de la actualidad (Rogel Vide, 2007). La esclavitud fue abolida en la segunda mitad del siglo XIX en países como España y Estados Unidos si bien, de acuerdo con EpData (2021), esta realidad sigue dándose hoy aun en ciertos países del continente africano -algunos ejemplos son Eritrea, Sudán del Sur y Burundi, entre otros- así como

en países asiáticos como Corea del Norte que encabeza la lista de los países con mayor prevalencia de la esclavitud.

Los Códigos civiles del siglo XX se retractan del abandono (Rodríguez Guitián, 1995) de los valores más importantes del hombre (De Castro y Bravo, 1959) y de la ausencia de regulación en materia de derechos de la personalidad de los anteriores códigos (Rodríguez Guitián, 1995), la cuando la protección civil de la persona ya se considera necesaria (De Castro y Bravo, 1959).

Rodriguez Guitián (1995) expone que, si bien la idea tradicional de la reparación del perjuicio moral era que se esto se trataba del comercio con la persona y por ende la ausencia de tutela civil, la jurisprudencia fue dando luz a este asunto dado que los Códigos civiles no se comprometían. Esta situación se dio en España por primera vez con la Sentencia del Tribunal Supremo de 6 de diciembre de 1912, admitiéndose por vez primera el perjuicio moral y su posibilidad de ser indemnizable con motivo de una lesión al honor la cual no estaba tipificada como delito o falta.

La pasada falta de atención hacia los derechos de la personalidad por parte de los civilistas europeos, cambió sustancialmente hacia una creciente preocupación por el asunto a partir del año 1947 (Rodríguez Guitián, 1995). En este sentido, la Segunda Guerra Mundial y todo lo ocurrido en ella fue transcendental para dar luz a la Declaración Universal de Derechos Humanos de 1948. En esta Declaración se reconoce el DHIPI, concretamente, en su artículo 12, por el cual se establece:

> "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Posteriormente, con la entrada en vigor de la Constitución Española en 1978 se recoge el DHIPI en su artículo 18.1, adquiriendo la consideración de derechos fundamentales. Pese a la escasez de antecedentes en las Constituciones modernas, afirma Puente Muñoz (1980) como la novedad en el reconocimiento del derecho a la intimidad personal y a la propia imagen dentro de nuestro ordenamiento jurídico se trataba de algo necesario.

Tal y como expone Londoño Toro (1987), tanto el concepto como la protección atribuida a los derechos de la personalidad ha variado a través del tiempo. Así, en la actualidad permite ser considerarlo también como un presupuesto para el ejercicio de otros derechos y libertades, y no únicamente como un límite negativo. En este sentido, jurisprudencialmente se ha tendido a extender el alcance de estos derechos. Como recalca

la sinopsis del artículo 18 CE realizada por el Congreso, un ejemplo de ello se da en los casos del derecho a la intimidad, concretamente, en el caso del derecho a la intimidad del domicilio cuando se da una situación de contaminación acústica u odorífera.

2.2. Conceptos de honor, intimidad y propia imagen.

La Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (en adelante, LOPH), no desarrolla una definición de estos conceptos, al igual que tampoco hace distinción entre los derechos y sobre cuál es el bien o interés jurídico que protegen (Calaza López, 2011).

Los derechos de la personalidad son un elemento no pecuniario del patrimonio. Se trata de un conjunto de derechos subjetivos contemplados por el ordenamiento jurídico, constituido por representaciones, ya sean físicas o psicológicas, de la persona los cuales tutelan la dignidad de esta (De la Parra Trujillo, 2014).

Debido a la singularidad de estos derechos y la conexión que mantienen entre ellos, la lesión de uno de ellos suele llevar aparejada la lesión conjunta de otro derecho fundamental de los recogidos en el mismo precepto constitucional. Como expone Calaza López (2011), esto se debe a su "'conflictiva relación jurídica', como consecuencia del libre ejercicio del derecho a la información y a la libertad de expresión o ideológica".

Sin embargo, a pesar del estrecho vínculo existente entre ellos, se trata de tres derechos diferenciados, por lo que no debemos olvidar la autonomía y sustantividad de estos tres derechos, tal y como recalca la STC 14/2003.

2.2.1. El concepto de derecho al honor.

El derecho al honor se encuadra dentro de la categoría de los conceptos jurídicos indeterminados debido a su falta de concreción no solo en la LOPH sino en todo el ordenamiento jurídico español.

Sin embargo, siguiendo la sinopsis del artículo 18 CE proporcionada por el Congreso, el derecho a honor ha gozado de protección en el ordenamiento jurídico español de forma tradicional al tratarse de uno de los "derechos clásicos de la personalidad".

Para la Real Academia Española (en adelante, RAE), el honor es la "cualidad moral que lleva al cumplimiento de los propios deberes respecto del prójimo y de uno mismo". En

este sentido, Serrano Martínez (1956) lo define por ello como un concepto espiritual e intrínseco a la persona, conexo íntimamente a la propia conciencia del individuo.

El honor es una noción dependiente y determinada por factores diversos, entre ellos, las normas, costumbres, ideas y valores sociológicos que estén presentes en cada instante histórico concreto dado que estos son cambiantes.

Sin embargo, como expone Calaza López (2011):

> "Ello no ha impedido al TC definirlo como el 'derecho al respeto y al reconocimiento de la dignidad personal que se requiere para el libre desarrollo de la personalidad en la convivencia social, sin que pueda (su titular) ser escarnecido o humillado ante uno mismo o ante los demás'". (p. 48)

2.2.2. El concepto de derecho a la intimidad.

Siguiendo lo establecido por la RAE, en su segundo precepto indica que la intimidad se trata de la "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

Por otro lado, Calaza López (2011) expone que el derecho a la intimidad, para la doctrina procesal actual puede interpretarse como aquel derecho al aislamiento o a no sufrir molestias de terceros y a tener privacidad.

Es propio individuo quien decide en qué medida exterioriza esta información relativa a su esfera privada. En este sentido, López Jiménez (2013) alude a la facultad del individuo para decidir "cuándo, cómo, de qué manera y frente a quién desvela esas situaciones, sucesos, hechos, datos, y/o sentimientos, que le pertenecen, que son suyos y de los que puede, por tanto, disponer". Así, la esfera de intimidad necesaria cambia para cada individuo en función de las circunstancias de este. Un ejemplo de esta exteriorización de la información que inicialmente podría considerarse íntima es el caso de las figuras públicas que dan a conocer voluntariamente ciertos aspectos de su vida privada.

Londoño Toro (1987) se refiere a este concepto desde el punto de vista jurídico, el cual se denomina *privacy* en el sistema anglosajón, para explicar su origen relativamente reciente. La protección estatal de la esfera privada, concretado en *right to privacy*, se inicia con el desarrollo teórico de Warren y Brandeis en 1890 para, posteriormente, experimentar una evolución gracias a la jurisprudencia y la legislación. En efecto, un ejemplo de este desarrollo es el artículo 12 de la Declaración Universal de los Derechos del Hombre de 1948 ya mencionado al exponer la trayectoria histórica del DHIPI.

El desenvolvimiento y protección del derecho a la intimidad experimenta grandes retos en la sociedad digital y de la información. Aquello que en principio presume de ser el derecho y la facultad del individuo de controlar su información personal y privada sobre las injerencias ajenas, compartiendo únicamente aquello que esta persona desea, sufre un descontrol en la Era de internet, perdiendo el control del destino y recepción de esta información. En este sentido, siguiendo a Gacitúa Espósito (2014), la protección frente a las intromisiones externas en la esfera privada del individuo ya no es la única función de este derecho, puesto que ahora se extiende al control efectivo y real del que dispone el individuo sobre su propia información personal.

La Era digital, producto de los avances tecnológicos llevados a cabo en las últimas décadas, ha dado paso a una reconceptualización del concepto de intimidad y de lo que se conoce como privacidad. De acuerdo con Lucena Cid (2014), si bien tradicionalmente la idea de privacidad se tomaba como aquello que implicaba la autonomía, el secreto, el desarrollo de la personalidad, entre otros términos, actualmente se toma más por aquella reivindicación por el control y protección de nuestra información personal frente a la injerencia de las nuevas tecnologías y el procesamiento, almacenamiento e, incluso, difusión de dicha información. Este control y protección que se defiende no es solo en términos cuantitativos sino también cualitativos -en lo que a la veracidad de la información se refiere y en el tipo de información del que se puede disponer-.

Comprobamos de esta forma, como se exponía anteriormente, que los conceptos concretos de los derechos de la personalidad se encuentran en constante evolución y como la concreción específica del término debe realizarse conforme al momento histórico con el que se esté tratando.

2.2.3. El concepto de derecho a la propia imagen.

En lo que a la propia imagen se refiere, nos referimos a la proyección física de la persona y que, por lo tanto, puede ser captada y reproducida por distintos medios -fotografía, vídeo, pintura, entre otros-.

Como expone De la Parra Trujillo (2014), este derecho adquirió una gran importancia con la invención de la fotografía puesto que posibilitaba la captación y reproducción de la imagen de la persona de forma arbitraria y sin consentimiento.

Así, la defensa del derecho a la propia imagen cobra su función en aquellos casos en los que se explotan los rasgos físicos de la persona. Como se exponía anteriormente, debido

al nexo existente entre estos tres derechos, la afectación al derecho a la propia imagen muchas veces va aparejada con la vulneración del derecho al honor o del derecho a la intimidad. Esta situación se da cuando la reproducción de la imagen de la persona conlleva una repercusión negativa para la reputación pública de la persona o cuando se trata de la divulgación de cuestiones de la vida privada del individuo.

Por ello, la regulación de este derecho ha ido evolucionando desde la pintura y escultura, hasta la actualidad, donde se empieza a hablar de creación de contenido por parte de la Inteligencia Artificial y de las técnicas de edición audiovisuales, las cuales permiten alterar la imagen y el sonido que se muestra en un vídeo o reproducción audiovisual. En este sentido, las técnicas de edición de video que facilitan la creación de "efectos especiales" y permiten rejuvenecer o envejecer a los actores o alterar sus voces.

Es más, la empresa londinense Flawless, ha desarrollado un *software* al que han llamado "TrueSync". Se trata de una invención galardonada con el premio "TIME Magazine Best Inventions of 2021", la cual permite realizar un doblaje visual de los vídeos -a lo que han llamado *vubbing*-, frente al doblaje tradicional -en inglés, *dubbing*- (cfr. Pastor, 2022). Dado que la imagen de la persona es manipulable, esta herramienta invita a reflexionar sobre todos sus posibles usos y las consecuencias de los mismos.

2.3. Concepto de derecho a la protección de datos.

Un derivado de la idea de privacidad es el control de la propia información y la facultad para decidir cuándo, cómo y en que extensión se facilita la información personal a terceros. Para Westin, siguiendo a Lucena Cid (2014), es lo que designa como "autodeterminación informativa".

La protección de datos es una actividad esencial en la era de las tecnologías de la información y comunicación, dónde el uso de datos masivos -en su término anglosajón, *Big Data*- y la comercialización de los datos muestra de forma candente la necesidad de desarrollar este tipo de salvaguarda para preservar el control de la información personal en equilibrio con las nuevas tecnologías.

De acuerdo con Puente Escobar (2008):

> "Es un derecho de configuración sumamente reciente, dado que sólo cabe hacer referencia con propiedad al mismo dentro de los últimos treinta o treinta y cinco años, y es un derecho cuya configuración se ha ido produciendo de forma progresiva, dentro de ese

> lapso al que acabamos de referirnos, de forma que sólo en las épocas más recientes ha sido reconocido universalmente como tal derecho fundamental". (p.14)

Por otro lado, Cardona Rubert (2014) define la protección de datos personales como:

> "La protección de datos de carácter personal es el conjunto de técnicas llamadas a dar soporte y garantizar el ejercicio del derecho a la autodeterminación informativa, concebido como la capacidad y derecho de los individuos de ejercer el control sobre las informaciones que les atañen" (p.1).

2.3.1. Qué entendemos por "dato".

De acuerdo con la RAE, la palabra "dato" tiene su procedencia etimológica en el latín, *datum*, que significa "lo que se da". Del origen y significado etimológico de esta palabra se puede interpretar que un dato no se puede simplemente deducir o insinuar, sino que, por lo general, ha de facilitarse.

Dentro del concepto de dato, encontramos aquellos datos calificados como de carácter personal. El Reglamento General de Protección de Datos (en adelante, RGPD), en el primer apartado de su artículo 4, proporciona una definición de lo que, a efectos de este Reglamento -y, por tanto, de la normativa relativa a la protección de datos- se entiende por datos personales o datos de carácter personal. En virtud de ello, se entenderá por datos personales que haga referencia las personas físicas y que permita identificar a las mismas, ya sea de forma directa o indirecta. Esta información abarca desde la información que se pueda recabar con el Documento Nacional de Identidad de la persona -nombre, número de identificación, domicilio, etc.- hasta, incluso, la información genética de la persona.

Dentro de la clasificación de los datos de carácter personal, encontramos una subcategoría especial de datos. Esta categoría se refiere a aquellos datos relativos a la salud, origen étnico o racial, ideología política, orientación sexual, confesión religiosa, entre otros datos considerados de carácter sensible.

A nivel de la normativa de producción nacional, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, la LOPDGDD) no proporciona una definición expresa de lo que debemos entender por datos personales. Esta Ley sí hace alusión a las categorías especiales de datos, donde se menciona qué tipo de datos comprende esta categoría, así como a los datos de naturaleza penal -aquellos datos personales relativos a condenas e infracciones

penales-. Sin embargo, la AEPD esclarece y define este concepto acudiendo a la definición proporcionada por el RGPD.

3. EL DERECHO AL HONOR, INTIMIDAD Y PROPIA IMAGEN.

3.1. Marco normativo europeo.

A nivel europeo encontramos una producción normativa muy relevante por formar parte de un marco de referencia básico.

En este sentido, resulta primordial la consideración del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, también conocido como Convenio Europeo de Derechos Humanos (en adelante, CEDH), el cual fue firmado por los Gobiernos miembros del Consejo de Europa.

Esta Declaración tiene como objetivo asegurar el reconocimiento y aplicación universal y efectiva de los derechos en ella desarrollados. Los Estados firmantes se comprometen a garantizar los derechos y libertades recogidos en este Convenio, así como todos los protocolos del mismo. A este respecto, siguiendo a Salado Osuna (1994), conforme con el protocolo de enmienda nº11 se instituye el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) como órgano único de garantía y control con carácter permanente. Además, este Tribunal tiene competencia para la interpretación y aplicación del CEDH.

En lo que respecta al DHIPI, se consagra en el artículo 8 del CEDH el derecho al respeto de la vida privada y familiar, estableciendo en su apartado primero que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y correspondencia". Además, en su apartado segundo, se establece las imposibilidad de injerencia en el ejercicio de este derecho por parte de las autoridades públicas salvo en aquellos casos previstos por ley y se trate de una situación de interés público.

Por otro lado, encontramos otro instrumento a nivel europeo fruto de los valores comunes de los países de la Unión Europeo que busca reforzar la protección a los derechos fundamentales. Este instrumentos es la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, CDFUE), cuyo artículo 7 consagra el respeto de la vida privada y familiar con una fórmula muy similar a la del artículo 8 del CEDH.

Además, resulta relevante mencionar que desde el Tratado de Lisboa de 2007 que modifica el Tratado de la Unión Europea (en adelante, TUE), el artículo 6 del TUE atribuye a la CDFUE el mismo valor jurídico que los Tratados. La consecuencia directa de ello es que los Estados miembros de la Unión Europea deberán acatar la CDFUE y proteger los derechos en ella recogidos. Asimismo, el contenido del CEDH también formará parte del Derecho de la Unión como principios generales.

De acuerdo con Cordero Álvarez (2012), en lo que respecta al derecho al honor, este parece no estar expresamente reconocido en el ámbito europeo, si bien cabe deducirse del artículo 10 del CEDH al establecerse este como límite al derecho a la libertad de expresión -bajo el término de "reputación ajena"-.

En una situación similar se encuentra el derecho a la propia imagen en el ámbito europeo dado que este no se encuentra reconocido expresamente. Sin embargo, este derecho es reconocido jurisprudencialmente en la aplicación del artículo 8 del CEDH por parte del TEDH como una manifestación del derecho a la intimidad (Blanco Martínez, 2016). En este sentido, Díez-Picazo (2021, p.295) cita la STEDH *Sciacca c. Italia* de 11 de enero de 2005 para exponer de qué forma este Tribunal no considera el derecho a la propia imagen como un derecho autónomo sino únicamente se protege para el caso en el que se encuentre conectado con la intimidad.

Se destaca también la reciente ampliación jurisprudencial del alcance del derecho a la intimidad. Así, esta protección se ha ido extendiendo a supuestos de agresiones ambientales como son los casos de contaminación acústica, odorífera o química, entre otros (cfr. Elvira Perales, 2003, "Sinopsis artículo 18"). Un ejemplo llamativo en relación con ello es la Sentencia del Tribunal de Estrasburgo sobre el caso *López Ostra c. España*, de 9 de diciembre 1994 en la que, de acuerdo con Bouazza Ariño (2015), se introduce una novedosa doctrina según la cual ciertas lesiones medioambientales graves pueden suponer una lesión a los derechos humanos.

Otro caso que destacar es el caso *Guerra y otros c. Italia*, de 19 de febrero 1998, por el cual el Tribunal declaró que los efectos de las emisiones de sustancias tóxicas y nocivas en grandes cantidades a la atmósfera atentaban contra el derecho a la intimidad del artículo 8 CEDH.

3.2. Marco normativo español.

Dentro de la regulación estatal de España para estos derechos encontramos dos fuentes principales. En primer lugar, la Constitución Española de 1978 en su artículo 18.1, cuyos derechos en él contenidos tienen rango de fundamentales. De esta forma, el artículo 18.1 CE consagra tres derechos fundamentales cuya finalidad última común es la protección de la vida privada de la persona. Así, este precepto establece: "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Por otro lado, la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, la cual, en mandato expreso del artículo 81.1 CE, desarrolla el artículo 18.1 CE.

Esta ley, en su artículo primero apartado tres califica estos tres derechos como irrenunciables, inalienables e imprescriptibles y, salvo en aquellos supuestos previstos por la propia ley, la renuncia a su protección será nula. Estos supuestos de renuncia se recogen en el segundo artículo de esta ley, de acuerdo con el cual no se dará una intromisión ilegítima cuando hubiese autorización legal expresa o el titular del derecho otorgase expresamente su consentimiento para ello. A pesar de ello, en el mismo precepto se indica respecto a este consentimiento que este "será revocable en cualquier momento, pero habrán de indemnizarse en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas". En esta línea, aquellos supuestos que, en el caso darse sin el consentimiento de su titular, reciben la consideración de intromisión ilegítima se encuentran recogidos de forma detallada en el artículo séptimo de la LOPDH (*vid.* Anexo I).

Adicionalmente, resulta necesario subrayar que estos derechos son de ejercicio personalísimo. Así, una concreción de ello es la exclusión de su ejercicio de entre las facultades de representación legal tienen los padres que ostenten la patria potestad respecto de sus hijos menores no emancipados (*vid.* Artículo 162 CC).

Por otra parte, como declara Alfaro Aguila-Real (1993, p.75): "normas como las contenidas en los arts. 6.2, 7.2 y 1255 CC establecen los límites a la autonomía privada traspasados los cuales el ordenamiento niega el reconocimiento a la actuación de los particulares". En este sentido, Díez-Picazo (2021, p.299) señala que estos derechos, dado que forman parte del orden público, se instauran como un límite a la autonomía de la voluntad del artículo 1255 CC por lo que, de acuerdo con esta afirmación, todo pacto, cláusula o condición contractual estipulado por los contratantes debe respetar estos derechos. Es por ello que la LOPDH regula, como se exponía *supra*, las cuestiones referidas al consentimiento de esta clase de intromisiones.

En lo que al **derecho a la intimidad** respecta, de acuerdo con la STC 231/1988, este derecho protege el "ámbito propio y reservado" de la persona, necesario para lograr una mínima calidad de vida (Díez-Picazo, 2021, p.284). Respecto a la delimitación del concepto de esfera privada, nuestro Tribunal Constitucional parece decantarse en la mayoría de sus sentencias por el criterio material, lo que implica que se entenderá por

íntimo aquello que, de acuerdo con las pautas sociales imperantes, se considere ajeno al interés de terceros (Díez-Picazo, 2021, p.285).

El derecho a la intimidad, como también ocurre para el derecho al honor y a la propia imagen, colisiona con otros derechos fundamentales como es el derecho fundamental a la libertad de expresión e información del artículo 20 CE. Este conflicto ha sido tratado por la jurisprudencia del Tribunal Supremo y del Tribunal Constitucional y, si bien cada situación debe examinarse de manera particular, los tribunales han fijado parámetros mediante la ponderación de derechos para que sirvan de orientación en su aplicación a cada circunstancia concreta (Elvira Perales, 2003, "Sinopsis artículo 20").

Resulta también relevante tener en cuenta las posibles injerencias a este derecho con origen en la relación jurídica laboral. A este respecto, Iberley (s.f.) recoge la doctrina del Tribunal Constitucional en la cual se traza el límite entre el necesario control de las comunicaciones electrónicas de los empleados por parte de la empresa y aquello que implicaría una injerencia en el derecho a la intimidad. En tal sentido, el Tribunal Supremo establece, como requisito de legitimidad de la actividad de control por parte del empresario, la superación de tres juicios: el juicio de "idoneidad", el de "necesidad" y el de "proporcionalidad".

En este sentido, siguiendo a Elvira Perales (2003, "Sinopsis artículo 18"), el derecho fundamental a la intimidad también entra en disputa en otras situaciones como son en las investigaciones de paternidad y maternidad (*vid.* STC 7/1994, de 17 de enero, donde el Tribunal Constitucional afirma respecto a este derecho que el mismo no se infringe cuando se trata de responder a limitaciones impuestas con motivo de deberes y relaciones jurídicas reguladas en nuestro ordenamiento, como es el caso de las pruebas biológicas para la determinación de la filiación).

En cuanto al **derecho al honor**, veníamos diciendo que se trata de la buena reputación de la persona. Respecto a esta afirmación, es el juez quien ha de valorar para cada caso en qué se concreta esta definición. Para ello, como se exponía en apartados anteriores, se debe atender a las costumbres y valores sociales imperantes, si bien también debe tenerse en cuenta, como indica Elvira Perales (2003, "Sinopsis artículo 18"), la relevancia pública de la persona afectada, cómo repercute la lesión en la vida profesional o en la privada, y el contexto concreto en el que se produce dicha lesión.

A este respecto, como muy acertadamente desarrolla Díez-Picazo (2021, p.296) para explicar la relación entre el derecho al honor y el derecho a la intimidad: "el honor es la

fachada exterior del edificio cuyo interior resguarda la esfera privada de la vida de las personas".

Pese a ser un derecho de carácter personalísimo, la jurisprudencia constitucional admite el ejercicio de este derecho por parte de los herederos de la persona que ha sufrido una injerencia a su derecho al honor cuando esta lesión transciende al ámbito familiar de estos (*vid*. STC 190/1996, de 25 de noviembre), así como también reconoce el derecho al honor de un pueblo o etnia (*vid.* El caso Violeta Friedman: STC 214/1991, de 11 de noviembre). De acuerdo con esto, estos afectados tendrían el interés legítimo que exige el artículo 162 CE para interponer el recurso de amparo (*cfr.* Díez-Picazo, 2021 y Elvira Perales, 2003, "Sinopsis artículo 18").

Respecto al **derecho a la propia imagen**, se configura como un derecho autónomo pese a su proximidad con el derecho a la intimidad y con el derecho al honor. De acuerdo con, Gómez Corona (2011), la jurisprudencia del Tribunal Constitucional define el objeto de este derecho y lo conecta con el honor y la intimidad al establecer que lo que este derecho salvaguarda es:

> "El interés del sujeto en evitar la difusión incondicionada de su aspecto físico, que constituye el primer elemento configurador de su intimidad y de su esfera personal y en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como individuo". (STC 99/1994, de 11 de abril).

Adicionalmente, debemos tener en cuenta que el derecho a la propia imagen protege aquello que permite reconocer e identificar a una persona concreta. Por lo cual, de acuerdo con Díez-Picazo (2021, p.293), además de la visión tradicional de este derecho por la cual se protege la imagen corporal, esto es, el aspecto físico de la persona, también se incluye en dicha protección la reproducción de la voz de la persona y el uso de la misma. En este sentido, la voz se incluye concretamente dentro de la protección otorgada por la LOPDH puesto que, de acuerdo con el apartado sexto de su séptimo artículo, tendrá consideración de intromisión ilegítima su uso para fines publicitarios, comerciales o de naturaleza análoga sin consentimiento expreso.

4. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS.

4.1. Marco normativo europeo.

Declara el Consejo de la Unión Europea (s.f.) en su artículo "Protección de datos en la UE" que "las normas de la UE sobre protección de datos son las más estrictas del mundo. En la UE se considera que la protección de datos personales es un derecho fundamental". Esto se ve reflejado en la producción normativa relativa a la protección de datos personales que se desarrolla a nivel europeo y el contenido de la misma.

La regulación relativa a la protección de datos a nivel europeo tiene como punto de arranque el Convenio 108 como el primer instrumento internacional jurídicamente vinculante relativo a la protección de datos. Esto Convenio se firma el 28 de enero de 1981 y, desde entonces, ha sido actualizado y ampliado por medio de sus distintos protocolos (Consejo de Europa, s.f., "Convenio 108 y Protocolos"). Posteriormente, el 23 de noviembre de 1995 introduce 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos, instrumento el cual supuso, en palabras de Rallo Lombarte en el libro "Tratado de Protección de Datos" (2019, p.24): "un hito en la historia de la protección de los datos personales no solo en Europa si no en el resto del mundo mediante la consagración de unos principios que todavía hoy tienen plena vigencia".

Siguiendo esta línea, la CDFUE cuenta con un artículo dedicado en exclusiva a este derecho. Así, el artículo 8 CDFUE versa lo siguiente:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Por otro lado, el Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) en su artículo 16 consagra también este derecho por medio de la siguiente fórmula:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

> 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
>
> Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea".

Tras la lectura de este precepto observamos el mandato establecido en el segundo apartado, por el cual se insta al Parlamento Europeo y al Consejo el desarrollo y aprobación de un marco normativo con regulación sobre esta materia. En este sentido, durante el inicio de la séptima Legislatura del Parlamento Europeo, la Comisión incluyó el *Data Protection Package* como parte de su programa. De acuerdo con López Aguilar (2015), con este paquete:

> "Se describe así un nuevo conjunto normativo compuesto de un Reglamento de Protección de Datos y una nueva Directiva reguladora de la garantía de la protección de datos ante las actuaciones policiales y judiciales de averiguación de delitos y enjuiciamiento de responsables" (p.30)

De esta forma, el Parlamento Europeo y el Consejo aprobaron el 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, denominado más sencillamente Reglamento General de Protección de Datos (en adelante, RGPD). El objetivo del mismo es, siguiendo lo declarado en las consideraciones preliminares del propio RGPD, garantizar un nivel coherente de protección sobre la materia en toda la Unión Europea y evitar las divergencias entre normativas que dificulten la libre circulación de datos personales dentro del mercado interior, creando para ello un régimen unificado para todos los Estados Miembros.

De acuerdo con Rallo Lombarte en su artículo "El nuevo derecho de protección de datos" (2019, p.56), "el Reglamento (UE) 2016/679 constituye un desarrollo completo y exhaustivo del derecho de protección de datos reconocido en el art. 8 CDFUE". Esto se debe a que, como el mismo autor recalca, la Directiva 96/46/CE, sustituida por el RGPD, no daba una respuesta adecuada a el avance tecnológico y a la globalización de la economía. Además, generaba una evidente ineficacia y desorden dentro del mercado

interior debido a la ausencia de normas comunes concretas que fuesen aplicables de forma homogénea en la Unión Europea. Afirma García Mahamut (2019, p.98) que "el paso cualitativo que da el RGPD es ese objetivo homogeneizador que quiebra el principio de territorialidad nacional así como la funcionalidad de las autoridades competentes a la hora de aplicarlo"

Por este motivo, el RGPD busca proporcionar una adecuación a los nuevos tiempos con un alcance general para todos los Estados Miembros de la Unión Europea, siendo directamente aplicable y de observancia imperativa en todos ellos. En cualquier caso, el RGPD deja libre un margen de maniobra de cara a la concreción por parte de los Estados Miembros de aquellos datos personales calificados de carácter sensible (Tomás Mallén, 2019, p.66).

En lo que al propio RGPD respecta, en su artículo primero apartado segundo califica el derecho de protección de datos personales como un derecho fundamental. Siguiendo con la protección proporcionada por este reglamento, en su artículo 5 se recogen los principios relativos al tratamiento de los datos personales los cuales se sintetizan en la obligatoriedad de que reciban un tratamiento lícito, leal y transparente, que sean recogidos para unos fines determinados y legítimos, que sean unos datos exactos y, en caso de ser necesario, estos deben actualizarse y, por último, se destaca también la necesidad de que los datos no sean mantenidos durante más tiempo del requerido para los fines del concreto tratamiento. Se ha de subrayar que la protección proporcionada por el RGPD alcanza a todas las personas físicas con independencia de su nacionalidad o lugar de residencia (Tomás Mallén, 2019, p.67), lo cual viene indicado en el artículo tercero del RGPD relativo al ámbito territorial de aplicación del mismo. Si bien, siguiendo a Megías Quirós (2019, p.150), el tratamiento de datos personales propios y ajenos llevados a cabo por una persona física no estará sujeto, por lo general, al RGPD para aquellos casos en los que se trate de actividades personales o domésticas y con objeto privado, a pesar de que se hayan podido efectuar en espacio público. El motivo de ello no es otro que salvaguardar el fin último de esta normativa, el cual es, como el mismo autor indica, "garantizar el derecho a la vida privada de los ciudadanos y al control de sus datos de carácter personal".

Estos requisitos del quinto artículo deben ser completados con el contenido del artículo 6 del mismo reglamento, el cual indica seis requisitos a cumplir mínimo uno para que el tratamiento sea lícito. Entre estas condiciones encontramos el otorgamiento del consentimiento del interesado, cuando el tratamiento de los datos es necesario para el cumplimiento de una obligación legal, o cuando este tratamiento es necesario por motivos

de interés público, entre otros. Estas condiciones resultan relevantes ya que guardan relación con los derechos del interesado derivados del tratamiento de los datos personales como pueden ser el derecho de rectificación y el derecho de supresión, entre otros, derechos los cuales serán objeto de análisis en secciones posteriores (*vid.* apartado 4.3. del presente Trabajo).

El RGPD también incorpora una regulación destinada a autoridades de control independiente, indicando las competencias, poderes y funciones de las mismas. En este sentido, siguiendo a García Mahamut (2019, p.100), con el RGPD se crea el Comité Europeo de Protección de Datos (en adelante, CEPD) cuyo antecedente inmediato es el GT29 de la Directiva 95/46/CE y cuya labor era la producción de *soft law* en materia de protección de datos (Cervera Navas, 2019, p.656). El precepto relativo a la creación de este organismo europeo es el artículo 68 RGPD de acuerdo con el cual, se compone por el Supervisor Europeo de Protección de datos y por cada uno de los directores de las autoridades de control de cada Estado miembro -en el caso de España, la Agencia Española de Protección de Datos (en adelante, AEPD)-. Una de las diferencias principales entre el CEPD y su antecedente es que este más reciente organismo tiene personalidad jurídica propia y naturaleza *sui generis*, indicado en el propio artículo 68 RGPD, dotando así de autoridad a sus dictámenes y de la posibilidad de adoptar decisiones jurídicas vinculantes (Cervera Navas, 2019, p.657). En este sentido, Megías Quirós (2019) referencia a la "Comunicación COM (2018) 43 final" de la Comisión Europea, en la que se indica:

> "'La interpretación del Reglamento compete a los órganos jurisdiccionales europeos (los tribunales nacionales y, en última instancia, el Tribunal de Justicia Europeo) y no a los legisladores de los Estados miembros', correspondiendo al nuevo Comité Europeo de Protección de Datos -sucesor del Grupo de Trabajo del artículo 29 (GT29)- emitir los dictámenes oportunos cuando sea necesario". (p.149)

De esta forma, el CEPD hereda muchas de las funciones que tenía su predecesor y, entre ellas, se destacan la formulación de orientaciones generales para informar sobre el RGPD y el asesoramiento a la Comisión Europea sobre aquellas cuestiones en materia de protección de datos y propuestas legislativas de la UE en relación con ello (Unión Europea, s.f., "Comité Europeo de Protección de Datos (CEPD)").

4.2. Marco normativo español.

Dentro de la normativa nacional respecto al derecho fundamental a la protección de datos encontramos, al igual que ocurría con el DHIPI, dos fuentes principales. En primer lugar, el precepto incluido en la Constitución Española de 1978, en su artículo 18.4; y, por otro lado, la regulación contenida en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Por lo tanto, en cuanto a la previsión constitucional de este derecho -también denominado derecho a fundamental a la autodeterminación informativa (STC 292/2000)-, comprobamos que la propia **Constitución Española** prevé en su artículo 18.4 que "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", declaración que sirve como punto de arranque del derecho a la protección de datos. Argumenta Díez-Picazo (2021, p.311) que, con esta redacción, si bien a priori puede parecer que el constituyente buscaba limitar el progreso tecnológico, lo que verdadera y lógicamente se buscaba es combatir los posibles abusos de derecho en el uso de las nuevas tecnologías.

Elvira Perales (2003) en su "Sinopsis artículo 18" subraya el hecho de que nuestra constitución es una de las primeras en introducir el derecho a la protección de datos frente al uso de la informática y la previsión evolutiva de la misma. De acuerdo con la autora, esto se debe a que "es precisamente en los años de su redacción cuando comienzan a apreciarse los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos".

La jurisprudencia constitucional ha expuesto en diversas sentencias la independencia de ente derecho frente a los otros apartados incluidos en el mismo artículo, tratándose de "un verdadero derecho fundamental, autónomo y claramente diferenciado de los demás" (Agencia Española de Protección de Datos, s.f., "Historia", en referencia a la STC 292/2000, de 30 de noviembre). Así, Díez-Picazo (2021, p.312) expone esto mismo recalcando la STC 254/1993, de 20 de julio, en la que se declara que el derecho fundamental a la protección de datos consiste en la "libertad frente a las potenciales agresiones a la dignidad y la libertad provenientes del uso ilegítimo del tratamiento mecanizado de datos, lo que la constitución llama 'la informática'".

Por otro lado, resulta importante mencionar que, de acuerdo con la STC 292/2000, de 30 de noviembre, la protección constitucional se extiende a todos los datos relativos a la

persona y no únicamente aquellos calificables de íntimos. De acuerdo con Serrano Pérez (2013), la misma sentencia señala lo siguiente:

> "Los poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la posibilidad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y su tratamiento, así como su uso, por un tercero, sea un poder público o un particular". (p.485)

En conexión con ello, pesar de la independencia del derecho fundamental a la protección de datos, este se encuentra estrechamente conectado con el derecho a la intimidad. En este sentido, la SAP Valencia 88/2013, de 12 de marzo expone que la "segunda dimensión de la intimidad conocida como libertad informática o *habeas data*, encuentra su apoyo en el art. 18.4 CE". La misma sentencia continúa desplegando la siguiente doctrina:

> "De esta proclamación se deriva su poder de acción del titular para exigir que determinados datos personales no sean conocidos, lo que supone reconocer un derecho a la autodeterminación informativa, entendido como libertad de decidir qué datos personales pueden ser obtenidos y tratados por otros. La llamada libertad informática significa, pues, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente (*habeas data*); en particular -como señala la doctrina- entre otros aspectos, la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (SSTC 11/98 de 13 de Enero y 45/99 de 22 de Marzo)".

Así, otros autores como Díez-Picazo (2021, p.313) exponen similarmente que, "la protección de datos comporta, ante todo, una facultad de acceso a los datos relativos a uno mismo. Así, haciendo un parangón con la venerable garantía de la libertad personal, se habla de *habeas data*". Define también Bazán (2005) el *habeas data* como lo siguiente:

> "Una acción, una garantía constitucional, un procedimiento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de los datos personales, frente a los posibles excesos del poder de registración precisamente de la información de carácter personal". (p.90)

Por todo ello, el *habeas data* sería un nuevo ejemplo de acción procesal destinado a fortalecer la situación jurídica de las personas en las sociedades tecnológicas (Pérez-Luño Robledo, 2017, p.36-47).

En lo que respecta la a **LOPDGDD**, la razón de la misma, como ley orgánica que es, es completar y dar desarrollo al derecho fundamental a la protección de datos previsto constitucionalmente. En este sentido, si bien los Reglamentos de la Unión Europea son de aplicabilidad directa, como bien se indica en el preámbulo III de la LOPDGDD, "en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de 'desarrollo' o complemento del Derecho de la Unión Europea".

En este sentido, expone Faya Barrios (2021, p.61) que con la publicación del RGPD se hizo evidente la necesidad de desarrollar una nueva ley de protección de datos en España, tanto para incorporar las novedades del RGPD, como para descargar de contenido la regulación nacional. Sin embargo, como bien indica el mismo autor (p.65): "existe una vocación clara del Reglamento europeo de convertirse en norma de cabecera, de aplicación cotidiana en el ámbito jurídico interno de los Estados miembros". Es por ello por lo que la LOPDGDD en gran parte de su articulado remite al RGPD de cara a conocer el contenido de determinados derechos, limitándose esta Ley a desarrollar, detallar o clarificar la forma de ejercicio de los derechos contenidos en el reglamento a nivel interno.

Es por ello por lo que en el artículo primero de esta Ley se indica el objeto de la misma, estableciendo su apartado a) que esta pretende adecuar nuestro ordenamiento jurídico al RGPD y completar las disposiciones de este, por lo que el marco normativo que vela por el ejercicio de este derecho fundamental se compone del RGPD y la LOPDGDD. Asimismo, el apartado b) de la Ley indica que la finalidad de la misma también incluye la garantía de los derechos digitales.

De la LOPDGDD resulta especialmente relevante hacer referencia a su Título VII en el cual se crea la AEPD. La creación de este ente se da, como se exponía anteriormente, con motivo de los criterios del Convenio 108 del Consejo de Europa relativo a la existencia de autoridades independientes de protección de datos (Agencia Española de Protección de Datos, s.f., "Historia"). Lo relativo a esta autoridad administrativa independiente se desarrollará en apartados posteriores (*vid*. sección 5 del presente Trabajo: "La Agencia Española de Protección de Datos), si bien cabe subrayar su importante papel a la hora de velar por el derecho fundamental a la protección de datos.

4.3. En particular, los derechos de los ciudadanos europeos en territorio español.

Tanto el RGPD a nivel europeo, como la LOPDGDD a nivel nacional, buscan en conjunto otorgar a los ciudadanos una serie de garantías con las cuales tener el control sobre sus propios datos personales. Estas garantías se concretan en una serie de derechos que puede ejercer cualquier persona física en relación con el tratamiento de sus datos personales (Grupo Ático34, s.f., "Derechos ARCO ¿qué son y cómo ejercerlos?"). Si bien para estos derechos no hay una ley que los desarrolle en exclusiva, estos se encuentran recogidos en el RGPD y en la LOPDGDD (Red Consultora Asociación, 2021, p. 23).

Así, a nivel europeo y a nivel nacional se desarrollan llamados Derechos "ARSULIPO" o "ARCO-POL". Este conglomerado de derechos se trata de una ampliación de los ya existentes Derechos "A.R.C.O." -un conjunto de derechos formado por los derechos de Acceso, Rectificación, Cancelación y Oposición-, ampliados por los Derechos "P.O.L." -en los cuales se incluye el derecho a la Portabilidad de datos, el derecho al Olvido y el derecho a la Limitación del tratamiento- siendo estos una de las principales incorporaciones del RGPD para adaptar los derechos ya existentes al nuevo contexto digital (*cfr*. Grupo Ático34, s.f., "Derechos ARCO ¿qué son y cómo ejercerlos?"; Red Consultora Asociación, 2021; *y* García Mahamut, 2019, p. 98). Resulta necesario precisar que el derecho de cancelación fue sustituido por el nuevo derecho de supresión en el marco de los nuevos derechos introducidos por el RGPD (Red Consultora Asociación, 2021, p.19).

De esta forma, en el Capítulo III del RGPD -denominado "derechos del interesado" y en el Título III de la LOPDGDD -llamado "derecho de las personas"- se desarrollan estos derechos introducidos en el párrafo anterior.

En resumidas cuentas, el conjunto de Derechos "ARSULIPO" está formado por los derechos de acceso, de rectificación, de supresión, derecho a la limitación del tratamiento, derecho a la portabilidad de los datos y derecho de oposición.

Resulta preciso subrayar que todos estos derechos se basan también en la obligación del responsable del tratamiento de los datos de asegurar un tratamiento leal y transparente (Puyol Montero, 2019, p.292). Este principio de transparencia e información en el tratamiento de los datos se encuentra recogido en los artículos 12 a 14 RGPD y en el artículo 11 LOPDGDD.

En la misma línea, siguiendo a Faya Barrios (2021, p.69-70), otros principios de protección de datos que resultan clave son, por un lado, el principio de exactitud de los

datos, el cual guarda conexión con el derecho de rectificación; por otro lado, también resulta especialmente relevante el deber de confidencialidad, el cual obliga a todos las sujetos que intervengan en el tratamiento de los datos personales, sin importar en qué fase lo hagan; y, por último, la necesidad de contar con el consentimiento del interesado cuando se pretenda tratar los datos para una pluralidad de fines, siendo necesario que el otorgamiento de dicho consentimiento para todos esos fines conste de manera "precisa e inequívoca".

4.3.1. El derecho de Acceso.

El derecho de acceso se encuentra recogido en el artículo 15 RGPD y en el artículo 13 LOPDGDD. De acuerdo con estos artículos, la AEPD (s.f., "Derecho de acceso") define este derecho como aquel por el cual toda persona puede dirigirse al responsable del tratamiento de sus datos personales para conocer si este los está tratando o no y, en caso de que se esté llevando a cabo dicho tratamiento, conocer, entre otras pesquisas: la finalidad del tratamiento, las categorías de datos que se estén tratando, el plazo previsto de conservación de los datos y los destinatarios de dicha información.

Asimismo, siguiendo a Puyol Montero (2019, p. 301), resulta de especial relevancia mencionar que tanto el derecho de acceso como el derecho de rectificación -el cual se desarrollará a continuación- se encuentran recogidos en la CDFUE en el apartado segundo del artículo 8 al disponer en la segunda parte de dicho apartado que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación".

4.3.2. El derecho de Rectificación.

El derecho de rectificación tiene una acepción polisémica. Por un lado, el artículo 20 CE, relativo al derecho fundamental a la libertad de expresión e información, ampara el derecho de rectificación el cual es desarrollado por la Ley Orgánica 2/1984, de 26 de mayo, reguladora del derecho de rectificación -en la cual, en su artículo primero se establece que toda persona "tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio"-. Por otro lado, el contenido en el RGPD y en la LOPDGDD (Grupo Ático34, s.f., "Derecho de rectificación, ¿qué es y cómo ejercerlo?")

Para el caso que nos concierne atendemos a la segunda acepción del término. Precisamente, el derecho de rectificación se encuentra recogido en los artículos 16 RGPD y 14 LOPDGDD. Dado que en la LOPDGDD se detalla el modo de ejercer este derecho, acudimos al RGPD para conocer el contenido específico del mismo. Así, artículo 16 RGPD, versa lo siguiente:

> "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".

De acuerdo con Adsuara (2019, p.315), este derecho se ha de poner en relación con los principios del artículo 5 RGPD relativos al tratamiento de los datos personales. Entre estos principios, el mismo autor presta especial atención al principio de exactitud de los datos, recogido en el apartado primero letra d). Dicho principio establece que los datos personales serán "exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".

4.3.3. El derecho de Supresión.

El artículo 17 RGPD y el artículo 15 LOPDGDD son los relativos al derecho de supresión -también denominado derecho al olvido-. Sobre este derecho, el RGPD indica una serie de circunstancias por las cuales "el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales". Así, este derecho proporciona una protección por la cual los interesados pueden solicitar que ante el responsable del tratamiento de los datos que este elimine sus datos personales (Red Consultora Asociación, 2021). Respecto a este derecho, expone Tomás Mallén (2019, p.77) la transcendencia de la STJUE de 13 de mayo de 2014, asunto C-131/12 relativa al caso *Google c. Agencia Española de Protección de Datos y Mario Costeja González*, sentencia en la cual se afirma el derecho al olvido digital y a la que siguen otras sentencias que confirman o matizan el mismo. La mencionada sentencia, de acuerdo con Santos Morón (2020, p.27), también establece que "cualquier tipo de operación que se realice con datos de naturaleza personal (recogida, registro, organización, conservación, consulta, comunicación a terceros, etc., cfr.art.4,2 RGPD) constituye un 'tratamiento de datos personales'".

Adicionalmente, resulta necesario mencionar la existencia de situaciones previstas en el RGPD en las cuales la supresión de los datos está prevista, más que como un derecho del interesado, como una obligación del responsable del tratamiento. De acuerdo con Adsuara (2019, p.321) estas situaciones son aquellos "tratamientos relacionados con la realización de determinadas operaciones mercantiles", "tratamientos con fines de videovigilancia" y los tratamientos en relación con los "sistemas de información de denuncias internas", entre otras.

4.3.4. El derecho a la Limitación del tratamiento.

De forma contigua, en el artículo 18 RGPD y en el artículo 16 LOPDGDD, encontramos el derecho de limitación de tratamiento. Este derecho conlleva la posibilidad de que los interesados soliciten la limitación en el tratamiento de sus datos personales cuando se dan determinadas condiciones. En virtud del artículo 18 RGPD, estas condiciones concretas son: (1) cuando haya duda sobre la exactitud de los datos tratados; (2) cuando, ante un uso ilícito, el interesado no desee que sus datos sean eliminados sino simplemente se solicite una limitación del uso de los mismos; (3) cuando el responsable del tratamiento ya no requiera del uso de dichos datos pero, por cuestiones jurídicas, estos no puedan ser eliminados; y (4) cuando el interesado se haya opuesto al tratamiento de los datos y dicha objeción esté pendiente de resolución.

De esta forma, tras la limitación del tratamiento, los datos del interesado solo podrán ser objeto de tratamiento en determinadas excepciones -como pueden ser, teniendo el consentimiento del interesado o por razones de interés público, entre otras-.

4.3.5. El derecho a la Portabilidad.

Seguidamente, en el artículo 20 RGPD y en el artículo 17 LOPDGDD se recoge el derecho a la portabilidad de los datos. Respecto a este derecho, el Grupo de Trabajo sobre Protección de Datos del Artículo 29 (en adelante, GT29) (2016, p.3-4), establece lo siguiente:

> "Este derecho permite a los interesados recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos. Este derecho, que se aplica bajo determinadas condiciones, respalda la elección, el control y la capacitación de los usuarios".

Así, la portabilidad de los datos supone una garantía para la recepción y traslado de los datos personales de acuerdo con los deseos del interesado, si bien este derecho "no se limita a los datos personales que son de utilidad y relevancia para servicios similares prestados por competidores del responsable del tratamiento" (GT29, 2016, p.7).

El autor Adsuara (2019, p.328) pone la lupa en el considerando 68 del RGPD el cual, en relación con el derecho a la portabilidad de los datos, establece lo siguiente:

> "Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato".

El mismo considerando indica que dicho derecho no debe aplicarse cuando el tratamiento sea necesario para el cumplimiento de una obligación legal por parte del responsable del tratamiento o cuando se trate del cumplimiento de un cometido de interés público.

4.3.6. El derecho de Oposición.

El derecho de oposición es el último de los derechos ARSULIPO. Se encuentra recogido en los artículos 21 RGPD y 18 LOPDGDD. De acuerdo con estos preceptos, el interesado tiene derecho a oponerse al tratamiento de sus datos personales en cualquier momento cuando este tratamiento sea lícito en base a que resulte "necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" (artículo 6.1.e) RGPD) o cuando este sea "necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero" (artículo 6.1.f) RGPD). Se incluye la elaboración de perfiles de acuerdo con estas condiciones.

Cuando estos casos se den, entonces el responsable del tratamiento deberá cesar el tratamiento de los datos personales. Sin embargo, de acuerdo con el RGPD, el responsable del tratamiento podrá continuar realizando dicho tratamiento cuando "acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".

Por otro lado, también se prevé en el apartado segundo que cuando este tratamiento tenga por objeto la mercadotecnia directa, el interesado podrá ejercer el derecho de oposición sobre sus datos personales en todo momento, inclusive cuando se realice para la

elaboración de perfiles en relación con dicha actividad. En el caso de ejercerse este derecho bajo esta motivación, el tratamiento de dichos datos deberá cesar.

Por otro lado, Adsuara (2019, p.331) destaca que el responsable del tratamiento de los datos cuenta también con su propio derecho de oposición frente al recurso de otro encargado. Esta previsión se encuentra en el artículo 28.2 RGPD, el cual establece lo siguiente:

> "El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios".

5. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

5.1. Origen de la entidad.

Las autoridades de control en materia de protección de datos, en general, y de la AEPD en concreto, se prevén por primera vez en el Convenio 108. Este Convenio, de acuerdo con Puente Escobar (2008, p.15), se trata del primer instrumento internacional que impone el establecimiento de una o varias autoridades en los Estados como requisito para garantizar el cumplimiento de la regulación del derecho fundamental a la protección de datos. En este sentido, menciona este mismo autor el artículo 13.2.a) de dicho Convenio, el cual establece que "cada Parte designará a una o más autoridades cuya denominación y dirección comunicará al Secretario general del Consejo de Europa". En cualquier caso, las funciones de dichas autoridades eran muy limitadas.

Siguiendo a Puente Escobar (2008, p.17), la siguiente fase llega en el marco de la Directiva 95/46/CE, en cuyo Considerando 62 se indica lo siguiente:

> "Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales".

La misma Directiva indica también en su Considerando 63 que "tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa". Además, la Directiva también impone un deber de colaboración y ayuda mutua entre las entidades de cada Estado miembro para lograr una protección en toda la UE y el deber de confidencialidad. Por último, se ampliaron las competencias de estas autoridades en comparación con otorgadas por el Convenio 108 predecesor (Puente Escobar, 2008, p.17-18).

En este marco, la AEPD se crea en 1992, si bien no comenzó a funcionar hasta 1994 (Agencia Española de Protección de Datos, s.f., "Historia"). Su creación se hizo mediante la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (Puente Escobar, 2008, p.24). En el apartado quinto de la exposición de motivos de esta Ley se indica que, con el fin de garantizar las disposiciones previstas en dicha ley, se "encomienda el control de su aplicación a un órgano independiente, al que atribuye el estatuto de Ente público en los términos del artículo 6.5 de la Ley General Presupuestaria". Posteriormente, en su Título VI se recoge la

regulación relativa este órgano especializado, estableciendo en el artículo 34.1 de la misma Ley: "se crea la Agencia de Protección de Datos" e indicando en el apartado segundo su carácter de independencia y configurándola como una entidad con personalidad jurídica propia.

En esta línea, la actual LOPDGDD, en el apartado primero de su disposición transitoria primera, se indica que este Estatuto de la AEPD "continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica", siendo dicho Título el relativo a los "procedimientos en caso de posible vulneración de la normativa de protección de datos". En este sentido, el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos fue derogado para dar paso al nuevo estatuto de la AEPD: el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

Con todo ello, la AEPD se configura como una autoridad independiente de control. Siguiendo a Rubí Navarrete (2019, p.492), en el Considerando 117 del RGPD se indica lo siguiente:

> "El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa"

Es por ello por lo que en el Título VII de la LOPDGDD se encuentra dedicado a las autoridades de protección de datos y, en concreto, el Capítulo I a la AEPD.

Además, el Considerando 119 establece que, en el caso de que un Estado miembro efectivamente establezca más de una autoridad de control, deben instaurarse mecanismos que garanticen la coherencia y participación efectiva de estas. En concreto, se deberá designar a una autoridad de control central que actúe como "punto de contacto único." En este sentido, España cuenta con "Agencias autonómicas" en Cataluña -la Autoridad Catalana de Protección de Datos-, País Vasco - la Agencia Vasca de Protección de Datos- y en Andalucía -el Consejo de Transparencia y Protección de Datos de Andalucía-; existía también una agencia en Madrid, si bien esta fue suprimida, asumiendo la AEPD sus funciones (Agencia Española de Protección de Datos, s.f., "Historia" *y* Rubí Navarrete, 2019, p. 504). Las disposiciones relativas a estas autoridades autonómicas de protección de datos se encuentran en la LOPDGDD en su Capítulo II.

5.2. Configuración y funciones de la entidad.

La AEPD se configura como el garante del derecho fundamental a la protección de datos (Puente Escobar, 2008, p.13). De acuerdo con el artículo 44.1 LOPDGDD:

> "La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones".

El artículo 47 LOPDGDD hace referencia a las funciones y potestades de la AEPD, entre ellas, la supervisión de la aplicación de la LOPDGDD y del RGPD. Este mismo artículo indica a su vez que, en particular, las funciones a realizar son las indicadas en el artículo 57 RGPD -el cual indica las funciones de toda autoridad de control en su correspondiente territorio-. Concretamente, entre dichas funciones encontramos: controlar la aplicación del RGPD y hacerlo aplicar, sensibilización del público y de los responsables en lo relativo al tratamiento de datos personales, facilitar a los interesados información en relación con el ejercicio de sus derechos y tratar las reclamaciones presentadas, entre otras (*vid.* Anexo II).

Por otro lado, para la realización de estas funciones, el artículo 58 RGPD indica una serie de potestades de las que disponen las autoridades de control para ejercer sus funciones. Estos poderes se dividen en tres bloques: poderes de investigación, poderes correctivos y poderes de autorización y consultivos (*vid.* Anexo III).

Junto a ello, siguiendo a Rubí Navarrete (2019, p.513), la LOPDGDD ha incluido una nueva competencia de la AEPD bajo la denominación "Potestades de regulación. Circulares de la Agencia Española de Protección de Datos" en el artículo 55, el cual versa lo siguiente:

> "La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán 'Circulares de la Agencia Española de Protección de Datos'.
>
> 2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado".

Expone este mismo autor como (p.514-516), frente al debate suscitado en relación con la naturaleza normativa o no y exigibilidad de las instrucciones que emitía la AEPD de acuerdo con la Ley precedente a la LOPDGDD, esta nueva ley establece expresamente en su tercer apartado la obligatoriedad de las circulares una vez publicadas en el Boletín Oficial del Estado.

Continuando con las competencias de la AEPD, Rubí Navarrete (2019) hace referencia a la siguiente novedad:

> "El reconocimiento de la posibilidad de activar procedimientos para la impugnación de una Decisión de la Comisión Europea en materia de transferencias internacionales de datos, siempre que la resolución de un procedimiento concreto dependiese de la validez de esa Decisión". (p.516)

De acuerdo con este autor, el fundamento de esta competencia se encuentra en los criterios expuestos por el TJUE en el caso *Maximillian Schrems c. Data Protection Commissioner*, de 6 de octubre de 2015 (C-362/2014) a raíz de la negativa de la autoridad independiente de protección de datos de Irlanda de tramitar una reclamación relativa a la trasferencia de datos personales por parte de la sociedad Facebook Ireland Limited -actualmente, "Meta Platforms Ireland Limited"- a Estados Unidos de acuerdo con la Decisión 2000/520/CE, de 26 de julio de 2000 de la Comisión, la cual fue adoptada conforme al artículo 25.6 de la Directiva 95/46/CE. La sentencia, en su consideración 15, indica que en la Comunicación COM (2013) 846 final, la Comisión señaló en el punto 3.2 "la existencia de diversas deficiencias en la aplicación de la Decisión 2000/520", señalando la existencia de empresas estadounidenses certificadas que no respetaban los denominados principios de puerto seguro. Por todo ello, el TJUE argumentó en su consideración 34 que la Decisión 2000/520 no se ajustaba a las exigencias derivadas de la CDFUE ni a los principios enunciados por el propio tribunal en otras sentencias. Finalmente, el TJUE, por todas las consideraciones desarrolladas en la sentencia, concluyó que la Decisión 2000/520 era inválida.

Siguiendo esto, Rubí Navarrete (2019, p. 517) indica que, pese a que el TJUE tiene competencia exclusiva en la declaración de invalidez de una acto de la UE, el Tribunal permite que las autoridades de control dispongan vías de actuación en estas situaciones. Así, la disposición adicional quinta de la LOPDGDD concreta esta novedosa competencia estableciendo:

"Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente".

6. PROBLEMÁTICA.

Como se introducía en la sección anterior, la AEPD ha de colaborar con la Administración de justicia en materia de protección de datos. En este sentido se abre la problemática de estudiar las respectivas competencias de cara a dilucidar la frontera entre la actividad de los tribunales civiles y de un ente administrativo como es la AEPD.

6.1. Los fines jurisdiccionales y no jurisdiccionales.

En primer lugar, es relevante considerar las disposiciones incluidas en la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial (en adelante, LOPJ). En este sentido, el artículo 236 octies LOPJ establece en su apartado segundo que:

> "Los tratamientos de datos con fines no jurisdiccionales estarán sometidos a la competencia de la Agencia Española de Protección de Datos, que también supervisará el cumplimiento de aquellos tratamientos que no sean competencia de las autoridades indicadas en el apartado anterior".

Por lo tanto, en primer lugar, observamos una distinción entre tratamientos de datos con fines jurisdiccionales y tratamientos de datos con fines no jurisdiccionales. En este sentido, el artículo 236 bis LOPJ indica en la segunda parte de su apartado primero que "tendrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional", por lo que los demás tratamientos serán con fines no jurisdiccionales. Establece el Consejo General del Poder Judicial (s.f.) que, para que el tratamiento se considere jurisdiccional, requiere dos elementos: (1) que los datos tratados estén anexos a un procedimiento judicial, y (2) que el fin de dichos tratamientos sea jurisdiccional, esto es, aquellos tratamientos "llevados a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes y el realizado dentro de la gestión de la Oficina judicial". Si estos requisitos no se cumplen, se tratará de un fin no jurisdiccional.

De acuerdo con el artículo 236 nonies LOPJ apartado primero, la autoridad de protección de datos para los tratamientos con fines jurisdiccionales es la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial.

En relación con ello, se establece en el artículo 236 decies LOPJ apartado primero:

> "Los tratamientos de datos llevados a cabo por el Consejo General del Poder judicial y la Fiscalía General del Estado en el ejercicio de sus competencias quedarán sometidos a lo

> dispuesto en la legislación vigente en materia de protección de datos personales. Dichos tratamientos no serán considerados en ningún caso realizados con fines jurisdiccionales".

Sabiendo esto, en el artículo 236 octies LOPJ apartado tercero establece:

> "El Consejo General del Poder Judicial, la Fiscalía General del Estado y la Agencia Española de Protección de Datos colaborarán en aras del adecuado ejercicio de las respectivas competencias que la presente Ley Orgánica les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia".

Por lo tanto, en el tratamiento de datos realizados por el Consejo General del Poder Judicial y de la Fiscalía General del Estado, que se considerará con fines no jurisdiccionales, deberán estas instituciones colaborar con la AEPD. El motivo de ello es que, cuando el tratamiento de los datos se efectúa en el ejercicio de funciones no jurisdiccionales, este se encuentra sometido al control de la AEPD y, en consecuencia, a las disposiciones del RGPD, LOPDGDD y su normativa de desarrollo (*vid*. artículo 236 quáter LOPJ).

6.2. La excepción doméstica.

Otro aspecto relativo al tratamiento y control de datos personales relevante es la llamada excepción doméstica. Esta previsión ya se incluía en la Directiva 94/46/CE predecesora del RGPD.

Este término es el que recibe la exclusión prevista en el artículo 2.2 RGPD al establecer: "El presente Reglamento no se aplica al tratamiento de datos personales: (…) c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas".

De esta forma, de acuerdo con Megías Quirós (2019, p.150) el tipo de tratamiento aquí expuesto sea de datos propios o ajenos, y se haya desarrollado en un ámbito privado o público, no estará sujeto al RGPD cuando tenga una finalidad privada. Esto se debe a que "la justificación de la excepción se encuentra en el fin último perseguido por la regulación, que es garantizar el derecho a la vida privada de los ciudadanos y al control de sus datos de carácter personal" (*Ibid.*, p.150).

En este sentido, el Considerando 18 del RGPD indica que: "entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades". Señala Megías Quirós (2019, p.150) la importancia

de que estos datos no se empleen para finalidades que excedan la función original de los mismos ya que, en caso de sobrepasar este cometido inicial, la excepción doméstica ya no sería de aplicación. Señala el Informe de la AEPD 0615/2008 (p.4) que, para darse la excepción doméstica, "es relevante que se trate de una actividad (…) equiparable a la que podría realizarse sin la utilización de Internet". En relación con esto, el mismo informe hace referencia a la SAN de 15 de junio de 2006 en la que se establecía que lo relevante no es la existencia de un tratamiento sino el ámbito o finalidad de dicho tratamiento. Por otro lado, la misma sentencia indicaba que el tratamiento de datos "será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos". Por consiguiente, el informe también señala que los ficheros mixtos -que comparten datos tanto personales como profesionales- no quedan amparados por la excepción doméstica y les sería de aplicación el RGPD, la LOPDGDD y su normativa de desarrollo.

Por todo ello, a modo de ejemplo, no será de aplicación la excepción doméstica en aquellas activades o publicaciones realizadas en páginas web de libre acceso para cualquier persona -como pueden ser las redes sociales-, cuando los datos se empleen en procedimientos judiciales, o cuando se les otorga un propósito o provecho comercial (Agencia Española de Protección de Datos, 2008 *y* Megías Quirós, 2018, p. 150).

Para el caso de las redes sociales en particular, indica Loza Corera (2021) que, ya el GT29 en su Dictamen 5/2009 sobre las redes sociales online, establecía que el tratamiento de datos realizados en este contexto muchas veces se corresponderán a casos contemplados en la excepción doméstica, si bien hay situaciones en las que no será así, como puede ser cuando la red social es empleada por una asociación o empresa, cuando el perfil de la red social es público -es decir, que el acceso al perfil del usuario va más allá de los contactos elegidos y todos los usuarios de dicha red social pueden tener acceso a los mismos-, o cuando "los datos son indexables por los motores de búsqueda".

Por último, resulta especialmente relevante para este Trabajo, lo establecido en el Informe 0615/2008 de la AEPD respecto a los casos en los que se acogen a la excepción doméstica:

> "No obstante, debe tenerse en cuenta que, si bien el derecho a la protección de datos puede no resultar de aplicación, si puede serlo la protección otorgada por otras normas frente a las intromisiones que supongan una vulneración de los derechos al honor, a la intimidad y a la propia imagen, que se regirá por lo dispuesto en la Ley Orgánica 1/1982, de 5 de

> mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen". (p.5)

6.3. La actividad de la jurisdicción civil.

De acuerdo con el artículo 9.2 LOPJ, "los Tribunales y Juzgados del orden civil conocerán, además de las materias que les son propias, de todas aquellas que no estén atribuidas a otro orden jurisdiccional". Además, en el artículo 52.1. 6º de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), establece:

> "En materia de derecho al honor, a la intimidad personal y familiar y a la propia imagen y, en general, en materia de protección civil de derechos fundamentales, será competente el tribunal del domicilio del demandante, y cuando no lo tuviere en territorio español, el tribunal del lugar donde se hubiera producido el hecho que vulnere el derecho fundamental de que se trate".

Recordamos que, al exponer el concepto de excepción doméstica, aquellos casos respaldados por esta excepción se sometían a la protección de la LOPDH. Como en la propia denominación de la ley se indica, esta protección es de carácter civil.

Las sentencias relativas al derecho fundamental a la protección de datos en el ámbito civil, en su mayoría van aparejadas con intromisiones ilegítimas al DHIPI. Así, en relación con el entorno digital, es relevante la STS 3212/2022 (Sala de lo Civil), de 28 de julio la cual trata el asunto de como la proyección no consentida de la imagen del demandante -con motivo de un reportaje emitido por la entidad demandada referente al narcotráfico en el que aparece el demandante como investigado- podía suponer una lesión contra el derecho a la propia imagen. Esta sentencia discutía la ponderación entre este derecho fundamental y el derecho fundamental a difundir información veraz, siendo el derecho a la información el prevalente en este caso particular como consecuencia de esta ponderación y debido a la importancia pública del caso sobre el que trataba el reportaje.

En cualquier caso, en lo que resulta relevante para nuestro caso esta sentencia es en la cita a la STC 27/2020, de 24 de febrero, en la que se hace referencia al impacto que implica el uso masivo de las nuevas tecnologías con respecto a los derechos fundamentales del artículo 18.1 CE y 18.4 CE. Esta sentencia señala que, con motivo del desarrollo tecnológico y del surgimiento de las redes sociales, los usuarios "han pasado de ser un sujeto pasivo receptor de información a un sujeto activo que elabora, modifica, almacena y comparte información". En esta sentencia también se expone en relación con

plataformas como “Facebook”, “Twitter” o “Instagram” la siguiente doctrina constitucional:

> “(i) Los usuarios de las redes sociales continúan siendo titulares de derechos fundamentales y su contenido sigue siendo el mismo que en la era analógica.
>
> (ii) El hecho de que circulen datos privados por las redes sociales en Internet no significa que lo privado se haya tornado público, puesto que el entorno digital no es equiparable al concepto de "lugar público" del que habla la Ley Orgánica 1/1982, ni puede afirmarse que los ciudadanos de la sociedad digital hayan perdido o renunciado a los derechos protegidos en el art. 18 CE.
>
> (iii) El reconocimiento constitucional de los derechos fundamentales comprendidos en el art. 18 CE, conlleva la potestad de la persona de controlar los datos que circulan en la red social y que le conciernen.
>
> (iv) Salvo que concurra una autorización inequívoca para la captación, reproducción o publicación de la imagen por parte de su titular, la injerencia en el derecho fundamental a la propia imagen debe, necesariamente, estar justificada por el interés público preponderante en tener acceso a ella y en divulgarla.
>
> (v) El titular del derecho fundamental debe autorizar el concreto acto de utilización de su imagen y los fines para los que la otorga. El consentimiento prestado, por ejemplo, para la captación de la imagen no se extiende a otros actos posteriores, como por ejemplo su publicación o difusión. De la misma manera, debe entenderse que la autorización de una concreta publicación no se extiende a otras, ya tengan la misma o diversa finalidad que la primigenia. Tampoco el permiso de uso otorgado a una persona determinada se extiende a otros posibles destinatarios. En definitiva, hay que entender que no puede reputarse como consentimiento indefinido y vinculante aquel que se prestó inicialmente para una ocasión o con una finalidad determinada”.

Por otro lado, la misma sentencia cita la STS 91/2017, de 15 de febrero, la cual señala que, pese a que el titular de un perfil accesible a todos usuarios de la plataforma haya publicado cierto contenido -por ejemplo, una fotografía suya-, ello no autoriza a un tercero a tomar dicho contenido y reproducirlo en otro medio de comunicación sin el consentimiento de su titular. El Tribunal menciona asimismo la reiterada jurisprudencia que establece que el consentimiento dado para la publicación de un contenido concreto para una finalidad determinada, no legitima la publicación de este contenido para finalidades distintas.

Resulta también relevante la STS 724/2023 (Sala de lo Civil), de 7 de febrero, en la cual trata una demanda sobre la tutela del derecho al honor por comunicación de datos

personales a un registro de morosos y por la inclusión indebida de la demandante en el mismo. En este litigio sobre la lesión al honor aparejada de una lesión al derecho a la protección de datos, resulta relevante el artículo 20.1 de la LOPDGDD, el cual establece:

> "Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:
>
> a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.
>
> b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.
>
> c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe"

Así, se estimaba que se habían cumplido los requisitos de este artículo por lo que "la comunicación al fichero de morosos de los datos personales relacionados con el impago de una deuda por razón del crédito del que es titular la demandada no constituye una intromisión ilegítima en el derecho al honor del demandante".

En cualquier caso, la tutela civil en materia de datos personales en exclusiva es escasa, si bien encontramos situaciones en las que el interesado acude a los tribunales civiles en lugar de ir a la AEPD para lograr una "imposición al responsable de una limitación o prohibición al tratamiento" (De Miguel Asensio, 2017, p.92). Un ejemplo de ello es el de la STS (Sala de lo Civil) 4162/2015, de 15 de octubre (*Ibid*.).

Por otro lado, fuera de la excepción doméstica, observamos que la tutela civil de este derecho tiende a ceñirse a la solicitud de indemnizaciones con motivo de la vulneración del RGPD. El artículo 82.6 RGPD prevé esto mismo al establecer: "las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2" en relación con el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento. Así, indica De Miguel Asensio (2017, p. 92) como "la interposición de una reclamación ante una autoridad de control no es una vía que permita obtener una reparación del daño, por lo que el ejercicio de acciones judiciales resulta necesario para hacer efectivo el derecho a indemnización". Este tipo de litigios contra la vulneración de

derechos con motivo del tratamiento de datos personales se suelen realizan ante los tribunales civiles (*Ibid*., p.92) salvo aquellos recursos contra resoluciones de la AEPD, que se llevan a cabo en el orden contencioso-administrativo -puesto que las resoluciones de esta ponen fin a la vía administrativa-.

6.4. La actividad de la AEPD.

Cuando se exponía la excepción doméstica, se mencionaba que, de acuerdo con el GT29 no cabía ampararse en ella cuando se trataba de un perfil público y accesible por todos los usuarios de la plataforma. Es en estos casos cuando actúa la AEPD en la defensa del derecho fundamental a la protección de datos.

Existen numerosos ejemplos de casos de difusión de datos personales en redes sociales. Ente ellos, se destaca el caso del Expediente nº PS/00158/2022, en el cual la parte reclamada publicó en su periódico "el audio de la declaración ante el juez de una víctima de una violación múltiple, para ilustrar la noticia de un caso muy mediático". La AEPD en sus resoluciones se sirve de la jurisprudencia de los tribunales de cara a solventar el caso. Así, la grabación de este caso trataba el relato realizado por la víctima -la cual era una persona anónima y no un personaje público- con una carga emocional sustancial y, sin negarse el derecho fundamental a la libertad de información, la AEPD expone que el TS en su sentencia (Sala de lo Civil) 697/2019, de 19 de diciembre, expresa:

> "La formación de una opinión pública libre no exige, ni justifica, que se afecte al derecho fundamental a la propia imagen (en este caso a la protección de datos personales) con esa gravedad y de un modo que no guarda la necesaria conexión con la identificación de la persona objeto de la información" (p.23)

Asimismo, la AEPD recuerda las obligaciones de los responsables del tratamiento de datos personales de acuerdo con el RGPD y la LOPDGG, especialmente "la responsabilidad proactiva, artículo 5.2 del RGPD, la valoración de los riesgos y la implementación de las medidas de seguridad adecuadas". Por otro lado, se hace referencia a los principios de protección de datos, indicando que el tratamiento de datos efectuado fue excesivo puesto que su uso no era necesario para el fin buscado por el periódico ya que, además, el hecho de facilitar esos datos no era de relevancia para la comunidad y únicamente buscaban "satisfacer la curiosidad"-. La sanción para estos casos es de una multa administrativa.

En este sentido, la Agencia Española de Protección de Datos en su "Listado de criterios comunes para la tramitación de quejas por parte de las Autoridades europeas de protección de datos" (2019), indica para estos casos la importancia de tener en cuenta los principios de protección de datos, en particular, el de la exactitud de los datos, de cara a valorar cada caso. Asimismo, es necesario que los datos sean relevantes de acuerdo con el interés público en tener acceso a la información y no excesivos.

Por otro lado, encontramos casos en los que la AEPD rechaza las reclamaciones interpuestas por considerarlas competencia de la jurisdicción civil. Algunos ejemplos de ello son el Procedimiento nº PS/00206/2019 (Recurso de Reposición nº RR/00774/2019) el cual trataba la resolución de la AEPD en un procedimiento sancionador por el tratamiento de datos realizado por un particular al "disponer de un dispositivo de obtención de imágenes de manera desproporcionada, tipificada en el art. 83.5a) RGPD, siendo sancionable de conformidad con el art. 58.2 b) RGPD". En concreto, el reclamado disponía de una instalación ilegal de una cámara de videovigilancia la cual captaba imágenes de forma constante de la vivienda de la recurrente, además, sin presencia alguna de un cartel informativo relativo a la instalación del dispositivo. La AEPD estima que dicho tratamiento no se ajusta a la normativa de protección de datos -la misma indica en la resolución inicial (p.2) que "los particulares pueden instalar cámaras de videovigilancia, si bien son responsables de que las mismas se ajusten a la legalidad vigente"- y que la instalación del dispositivo podía afectar a la intimidad. Sin embargo, la AEPD (p.4) estima que la resolución relativa a la intromisión en el derecho a la intimidad ha de ser la jurisdicción civil "la que determine la presunta conducta infractora por la afectación al derecho a la intimidad, tras respetar los derechos fundamentales del denunciado reconocidos en la normativa en vigor". Se encuentran numerosas otras resoluciones similares a esta, como pueden ser la resolución con Expediente nº EXP202204806 y la resolución del Procedimiento nº TD/00114/2019 (Recurso de Reposición nº RR/00440/2019).

Cabe destacar que, de acuerdo con la Agencia Española de Protección de Datos (2018), la videovigilancia se considera un tipo de tratamiento de datos de carácter personal puesto que se da la captación de imágenes de personas.

Resulta también relevante el caso del Procedimiento nº TD/00114/2019 (Recurso de Reposición nº RR/00440/2019) en relación con el ejercicio del derecho de supresión de unas URLs. La reclamación es desestimada por la AEPD al establecer que:

> "(…) debería haber interpuesto la reclamación contra la misma entidad que solicitó la supresión de las URLs, o bien ejercitar el derecho ante la entidad contra la que interpone la reclamación y en caso de que no recibiese contestación o esta fuera insatisfactoria, puede presentarse reclama ante esta Agencia Española de Protección de Datos" (p.5)

Sin embargo, en los hechos, el reclamante describe:

> "Dado la relación que el reclamante mantiene con reclamado, tras una reunión con la directora jurídica de la entidad, el medio desindexó la URL que dañaba la imagen del reclamante, pero sigue apareciendo en la hemeroteca, permitiendo a que cualquier persona pueda acceder a ella para dañar la imagen y que juega un papel importante en la vida profesional" (p.1)

Sin embargo, la AEPD continúa desestimando la causa, redirigiendo el reclamante a la jurisdicción civil dado que, en caso de que la petición de este sea la protección de su derecho al honor y a la propia imagen, debe acudir a la protección otorgada por la LOPDH. Por lo que, bajo esta premisa, la AEPD no es competente para dicha materia.

Seguidamente, la AEPD hace referencia a la SAP de 24 de febrero de 2011, indicando la necesidad de desvincular lo relativo a la protección de datos con aquella materia relativa al DHIPI cuya protección se recoge en la LOPDH, en cuyo artículo primero hace referencia a la protección civil del mismo. Por todo ello, la AEPD defiende que:

> "La LOPD se aplica en los supuestos en los que se hace necesario someter a determinados controles el empleo de los datos personales para evitar usos incontenidos, excesivos o destinados a fines contrarios a los recogidos o el tratamiento de los datos sin la información precisa etc. Todo esto se protege en un ámbito jurídico que es diferente a la divulgación de informaciones atentatorias a determinados derechos fundamentales como son el honor o el derecho a la propia imagen. La separación de ambos sistemas de protección se aprecia, también, por el hecho de que los preceptos que se aplican en ambos casos son diferentes y, además, los procedimientos previstos para la reacción ante la violación de uno y otro ámbito del ordenamiento jurídico también son diferentes" (p.2-3)

A pesar de ello, encontramos casos de colisión en la actividad de la AEPD y de los Tribunales civiles y constitucionales inclusive. Ejemplos de ello son los casos de resoluciones como la del Expediente nº EXP202209442 de la AEPD por la cual se estudia el caso de la instalación de unas cámaras de videovigilancia sin que se mostrase un cartel indicando la presencia de estas y el modo de ejercicio de los derechos de rectificación, supresión y demás derechos de los usuarios. En expediente, la AEPD entra a resolver este caso, procediendo a la apertura de un expediente sancionador de acuerdo con la normativa del RGPD y la LOPDGDD, por el cual se dispone que los hechos suponen una

vulneración a los establecido en la normativa de protección de datos -no informar acerca del tratamiento de los datos personales - e imponiendo la procedente multa administrativa.

7. CONCLUSIONES.

El DHIPI y el derecho fundamental a la protección de datos se encuentran estrechamente relacionados. Esto se debe solo por estar recogidos en el mismo precepto constitucional -en el artículo 18 CE- sino también a los numerosos casos en los que una intromisión en el derecho fundamental a la protección de datos -configurado como autónomo- puede suponer, a su vez, una intromisión en los derechos del artículo 18.1 CE.

La AEPD se trata de una autoridad administrativa independiente, competente para resolver las materias relativas a la protección de datos de carácter personal y, en caso de darse una intromisión ilegítima en este derecho fundamental, imponer sanciones que, en todo caso, tendrán carácter administrativo.

Por lo tanto, nos encontramos con que, por mandato de la normativa europea, una entidad de la administración estatal, que no el poder judicial, entra a resolver casos relativos a derechos fundamentales. La normativa europea asigna esta función a las autoridades de protección de datos con la finalidad de homogeneizar la aplicación del RGPD en toda la UE y sanar las divergencias producidas debido a los defectos de las normativas precedentes. Estas autoridades, además de contar con las potestades como autoridad de control, de acuerdo con el artículo 55 LOPDGG, se les otorga potestades de regulación por medio de disposiciones -las de la AEPD llamadas Circulares- las cuales son dictadas por la presidencia de la AEPD, siendo estas imperativas una vez publicadas en el BOE. En este sentido, la AEPD ha publicado la Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

En cuanto al análisis de la actividad realizada por parte de la jurisdicción civil y de la AEPD, podemos observar como la propia AEPD desestima aquellos recursos que considera competencia de los tribunales civiles. Si bien el RGPD "no incluye mecanismos de coordinación entre la tutela civil y la supervisión administrativa" (De Miguel Asensio, 2017, p.92), en materia de protección de datos, sumando a aquellos casos en los que se trata de reclamaciones indemnizatorias, comprobamos que son competencia civil aquellos casos que se acogen a la llamada excepción doméstica y aquellos en los que, si bien puede haber una lesión al derecho fundamental a la protección de datos, el derecho mayormente

lesionado es un de los derechos del artículo 18.1 CE y, por ello, se debe acudir a la jurisdicción de los tribunales civiles.

En cualquier caso, en el marco del derecho administrativo se trata un concepto llamado "huida del derecho administrativo" para exponer el fenómeno por el cual "las Administraciones públicas sujetan su actuación al Derecho privado o al Derecho laboral o adoptan personificaciones jurídico-privadas, alejándose de los controles y garantías del procedimiento administrativo, todo ello para lograr mayor flexibilidad en su actuación" (La Ley, s.f.).

Partiendo de este concepto, el fenómeno que nos concierne, que es, el hecho de que la tutela de un derecho fundamental -el derecho fundamental a la protección de datos- se lleve a cabo por un ente de derecho público, se podría asimilar a el suceso descrito en el párrafo anterior y, por ello, como una suerte de "huida del derecho civil" o "huida de la tutela civil". Puesto que se trata de un derecho fundamental, y por lo tanto su normativa desarrollo se realiza por vía de Ley Orgánica, la tutela de este correspondería a los Tribunales como ocurre con el DHIPI y, sin embargo, no se da de este modo.

Otros autores han empleado términos similares para a ver referencia a manifestaciones similares a las descritas en el párrafo anterior. Por ejemplo, Vélez Toro (2021) acuña el término "huida del proceso civil" para referirse a la dificultad de acceso al proceso civil con motivo de las sucesivas reformas de la LEC -ya fuese debido a los métodos alternativos de resolución de conflictos o ya fuese por restricciones directas al proceso- y como ello puede lesionar el derecho fundamental a la tutela judicial efectiva.

En cualquier caso, el fenómeno al que se refiere este Trabajo para ilustrar la actividad de la AEPD con respecto al derecho fundamental a la protección de datos, no se considera en cualquier caso que dañe este derecho fundamental en modo alguno. A más decir, podría decirse que este ente garantiza una mayor eficiencia en la salvaguarda de este derecho, al dedicar su actividad en exclusiva a su protección. En contraste con ello, de ser la jurisdicción civil la que otorgase esta protección, sus sentencias llevarían más tiempo debido la gran cantidad de asuntos que conoce y, en la sociedad como la actual, una demora en resolver estos asuntos puede provocar lesiones incluso irreparables en las personas -como ejemplo, la velocidad de difusión de los contenidos en Internet y la dificultad de rastreo y eliminación de ciertos contenidos-.

Finalmente, la accesibilidad de la vía administrativa frente a la vía civil fomenta que los reclamantes acudan a esta primera. La vía de la reclamación administrativa se encuentra

“sometida a menores costes y esfuerzos para el reclamante que el ejercicio de acciones judiciales” (De Miguel Asensio, 2017, p.91), lo cual facilita la solicitud de protección de este derecho fundamental por parte de los afectados.

8. BIBLIOGRAFÍA Y ANEXOS.

Adsuara, B. (2019). Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento). En Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos* (313-352). Tirant lo Blanch.

Agencia Española de Protección de Datos. (s.f.). Derecho de acceso. Recuperado el día 28 de marzo de https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-acceso

Agencia Española de Protección de datos. (2004). *Guía del derecho fundamental a la protección de datos de carácter personal*. https://datos.redomic.com/Archivos/GuiasUtiles/G33.pdf

Agencia Española de Protección de Datos. (s.f.). Historia. Recuperado el 27 de marzo de https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia

Agencia Española de Protección de Datos. (2008). Informe 0615/2008. https://www.aepd.es/es/documento/2008-0615.pdf

Agencia Española de Protección de datos. (2017). *Protección de Datos: Guía para el ciudadano*. https://www.aepd.es/es/documento/guia-ciudadano.pdf

Agencia Española de Protección de datos. (2018). Informe jurídico RGPD sobre interés legítimo. https://www.aepd.es/es/documento/informe-juridico-rgpd-interes-legitimo.pdf

Agencia Española de Protección de Datos. (2019). Listado de criterios comunes para la tramitación de quejas por parte de las Autoridades europeas de protección de datos. Recuperado el 9 de abril de https://www.aepd.es/sites/default/files/2019-09/criterios-gt29-wp225.pdf

Alfaro Aguila-Real, J. (1993). Autonomía privada y derechos fundamentales. *Anuario de Derecho civil*, 46 (1), 57-122.

https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1993-10005700122

Bazán, V., (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. *Estudios Constitucionales*, 3(2), 85-139. http://www.redalyc.org/articulo.oa?id=82030204

Blanco Martínez, E.V. (2016). Derecho a la propia imagen. Límites. Posibilidad de revisar la cuantía de la indemnización. En Yzquierdo Tolsada (Dir.), *Comentarios a las sentencias de unificación de doctrina: civil y mercantil* (319-334). https://www.boe.es/biblioteca_juridica/comentarios_sentencias_unificacion_doctrina_civil_y_mercantil/abrir_pdf.php?id=COM-D-2013-20

Bouazza Ariño, Omar. (2015). Medio ambiente e intimidad en la jurisprudencia del Tribunal Europeo de Derechos Humanos. *Ambienta*, (113), 92.107. https://www.mapa.gob.es/ministerio/pags/Biblioteca/Revistas/pdf_AM%2FPDF_AM_Ambienta_2015_113_92_107.pdf

Calaza López, S. (2011). Delimitación de la protección civil del derecho al honor, a la intimidad y a la propia imagen. *Revista de Derecho UNED*, (9), 43-59. http://e-spacio.uned.es/fez/eserv/bibliuned:RDUNED-2011-9-5030/Documento.pdf

Cardona Rubert, M.B. (2014). Protección de datos personales. *Diccionario internacional de derecho del trabajo y de la seguridad social*, 1809-1811.

Cervera Navas, L. (2019). El Comité Europeo de Protección de Datos. En Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos* (655-670). Tirant lo Blanch.

Consejo de Europa. (s.f.). Convenio 108 y Protocolos. Recuperado el 25 de marzo de https://www.coe.int/es/web/data-protection/convention108-and-protocol

Consejo de la Unión Europea. (s.f.). Protección de datos en la UE. Recuperado el 25 de marzo de https://www.consilium.europa.eu/es/policies/data-protection/

Consejo General del Poder Judicial. (s.f.). Tipos de tratamientos de datos en la Administración de Justica. Recuperado el 5 de abril de https://www.poderjudicial.es/cgpj/es/Temas/Autoridad-de-control-de-proteccion-de-datos/Proteccion-datos-en-Justicia/Tipos-de-tratamientos/

Cordero Álvarez, C.I. (2012). *La protección del derecho al honor, a la intimidad y a la propia imagen en el tráfico privado internacional* [Tesis doctoral, Universidad Complutense de Madrid]. E-Prints Complutense. https://eprints.ucm.es/id/eprint/16299/1/T33950.pdf

De Castro y Bravo, F. (1959). Los llamados derechos de la personalidad. *Anuario de derecho civil*, 12 (4), 1237-1276. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1959-40123701276

De la Parra Trujillo, E. (2014). *El derecho a la propia imagen*. Tirant Lo Blanch. https://www.tirantonline.com/cloudLibrary/ebook/info/9788490536353

De Miguel Asensio, P.A. (2017). Competencia y derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea. *Revista Española de Derecho internacional*, 69 (1), 75-108. http://www.revista-redi.es/wp-content/uploads/2018/01/3_estudios_miguel_asensio_competencia_dcho_aplicable_en_reglamento_general.pdf

Díez-Picazo, L.M. (2021). Los derechos de la vida privada. En Díez-Picazo, L.M., *Sistema de Derechos Fundamentales* (283-317). Tirant Lo Blanch.

Echeverría Muñoz, D. (2020). El derecho al honor, la honra y buena reputación: antecedentes y regulación constitucional en el ecuador. *Ius Humani. Revista de Derecho*, 9 (1), 209-230. https://doi.org/10.31207/ih.v9i1.228

Elvira Perales, A. (2003). Sinopsis artículo 18. *Congreso de los Diputados*. https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

Elvira Perales, A. (2003). Sinopsis artículo 20. *Congreso de los Diputados*. https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=20&tipo=2

EpData. (2021). La esclavitud en el mundo, en datos y gráficos. *EpData*. https://www.epdata.es/datos/esclavitud-mundo-datos-graficos/338

Faya Barrios, A.L. (2021). El contexto normativo en materia de protección de datos personales en derecho español. En Murga Fernández, J.P., Fernández Scagliusi, M.A. y Espejo Lerdo de Tejada, M. (Dir.), *Cuestiones actuales sobre protección de datos en España y México* (19-96). Tirant lo Blanch

Gacitúa Espósito, A.L. (2014). *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (En busca del equilibrio entre la libertad y la seguridad)* [Tesis doctoral, Universidad Autónoma de Barcelona]. Depósito Digital de Documentos de la UAB. https://hdl.handle.net/10803/284352

García Mahamut, R. (2019). Del Reglamento General de Protección de Datos Personales y Garantías de los Derechos Digitales. En García Mahamut, R. y Tomás Mallén, B. (Eds.), *El Reglamento General de Protección de Datos*. Tirant lo Blanch.

Gómez Corona, E. (2011). Derecho a la propia imagen, nuevas tecnologías e internet. En Cotino Hueso, L. (Coord.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (444-466). Universidad de Valencia. http://hdl.handle.net/11441/63443

Grupo Ático34. (s.f.). Derechos ARCO, ¿qué son y cómo ejercerlos?. *Grupo Ático34*. https://protecciondatos-lopd.com/empresas/derechos-arco-que-son/

Grupo Ático34. (s.f.). Derecho de rectificación, ¿qué es y cómo ejercerlo?. *Grupo Ático34*. https://protecciondatos-lopd.com/empresas/derecho-rectificacion/

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (2009). *Dictamen 5/2009 sobre las redes sociales en línea.* https://www.aec.es/wp-media/uploads/DPD-00207.pdf

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (2016). *Directrices sobre el derecho a la portabilidad de los datos.* https://www.aepd.es/sites/default/files/2019-09/wp242rev01-es.pdf

Iberley. (s.f.). Derecho a la intimidad de la persona trabajadora. *Iberley*. https://www.iberley.es/temas/derecho-intimidad-persona-trabajadora-64287

La Ley (s.f.). Huida al derecho privado. *Guías jurídicas La Ley*. https://guiasjuridicas.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUMjCxMTtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAGMNmyzUAAAA=WKE

Londoño Toro, B.S. (1987). El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas. *Revista Facultad de Derecho y Ciencias Políticas*, (77), 107-146. https://dialnet.unirioja.es/servlet/articulo?codigo=5460991

López Aguilar, J.F. (2015). Data Protection Package y el Parlamento Europeo. En Rallo Lombarte, A. y García Mahamut, R. (Eds.), *Hacia un nuevo derecho europeo de protección de datos* (29-81). Tirant lo Blanch

López Jiménez, D. (2013). Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español. *Estudios Constitucionales*, 11(2), 575-614. https://www.redalyc.org/articulo.oa?id=82029345015

Loza Corera, M. (1 de febrero, 2021). Sobre la "Excepción Doméstica". *Asociación Española para la Calidad*. https://dpd.aec.es/sobre-la-excepcion-domestica/

Lucena Cid, I.V. (2014). El concepto de la intimidad en los nuevos contextos tecnológicos. En A. Galán Muñoz (Coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación* (15-54). Tirant Lo Blanch. https://www.tirantonline.com/cloudLibrary/ebook/show/9788490537657

Megías Quirós, J.J. (2019). RGPD y actividades personales en materia de protección de datos. *Persona y Derecho*, 80, 147-178. https://doi.org/10.15581/011.80.147-178

Pastor, J. (22 de diciembre, 2022). El doblaje de películas tiene un problema, se llama inteligencia artificial y ya tiene alucinantes resultados. *Xataka*. https://www.xataka.com/cine-y-tv/doblaje-peliculas-tiene-problema-se-llama-inteligencia-artificial-tiene-alucinantes-resultados

Pérez-Luño Robledo, E.C. (2017). *El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías*. Dykinson.

Puente Escobar, A. (2008). La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal, *Azpilcueta*, (20), 13-41. https://core.ac.uk/display/11501783?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

Puente Muñoz, T. (1980). El derecho a la intimidad en la Constitución. *Anuario de derecho civil*, 33 (4), 915-928. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1980-40091500928

Puyol Montero, J. (2019). Transparencia de la información y derecho de acceso de los interesados en la nueva normativa de protección de datos. En Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos* (275-312). Tirant lo Blanch.

Rallo Lombarte, A. (2019). El nuevo derecho de protección de datos. *Revista Española de Derecho Consitucional*, 116, 45-74. https://doi.org/10.18042/cepc/redc.116.02

Rallo Lombarte, A. (2019). Del derecho a la protección de datos a la garantía de nuevos derechos digitales. En Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos* (23-52). Tirant lo Blanch.

Real Academia Española. (s.f.). Dato. En *Diccionario de la lengua española*. Recuperado el 28 de enero, 2023, de https://dle.rae.es/dato

Real Academia Española. (s.f.). Honor. En *Diccionario de la lengua española*. Recuperado el 27 de diciembre, 2022, de https://dle.rae.es/honor

Real Academia Española. (s.f.). Intimidad. En *Diccionario de la lengua española*. Recuperado el 27 de diciembre, 2022, de https://dle.rae.es/intimidad

Red Consultora Asociación. (2021). *Ley de Protección de datos para entidades y colectivos ciudadanos*. Ayuntamiento de Madrid. https://www.madrid.es/UnidadesDescentralizadas/Cooperacion-PublicoSocial/Formacion/Asociacionismo_Formacion/2021/Ficheros/LeyProteccionDatos.pdf

Rodríguez Guitián, A.M. (1995). *El derecho al honor de las personas jurídicas* [Tesis doctoral, Universidad Autónoma de Madrid]. Biblos e-Archivo. http://hdl.handle.net/10486/4340

Rogel Vide, C. (2007). Origen y actualidad de los derechos de la personalidad. *IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., (20), 260-282.* https://doi.org/10.35487/rius.v1i20.2007.278

Rubí Navarrete, J. (2019). La Agencia Española de Protección de Datos. En Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos* (491-520). Tirant lo Blanch.

Salado Osuna, A. (1994). El protocolo de enmienda nº11 al Convenio Europo de Derechos Humanos. *Revista de Instituciones Europeas*, 21(3), 943-966. https://www.cepc.gob.es/sites/default/files/2021-12/28324rie021003231.pdf

Santos Morón, M.J. (2020). Tratamiento de datos, sujetos implicados, responsabilidad proactiva. En González Pacanowska, I. (Coord.), *Protección de datos personales*. Tirant lo Blanch.

Serrano Martínez, E. (1956). “Honneur” y “Honor”: su significación a través de las literaturas francesa y española (Desde los orígenes hasta el siglo XVI). *Anales de la Universidad de Murcia. Filosofía y Letras*, 14 (3), 47-191. https://digitum.um.es/digitum/bitstream/10201/21702/1/02%20Honneur%20y%20Honor.pdf

Serrano Pérez, M.M. (2013). Los derechos al honor, a la intimidad personal y familiar y a la propia imagen. La inviolabilidad del domicilio. La protección de datos. En García Guerrero, J.L. (Dir.), *Los derechos fundamentales: la vida, la igualdad y los derechos de libertad*. Tirant lo Blanch.

Tomás Mallén, B. (2019). Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+ del Consejo de Europa. En García Mahamut, R. y Tomás Mallén, B. (Eds.), *El Reglamento General de Protección de Datos*. Tirant lo Blanch.

Unión Europea. (s.f.) Comité Europeo de Protección de Datos (CEPD). Recuperado el 25 de marzo de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/edpb_es

Vélez Toro, A.J. (2021). La huida del proceso civil. *Revista General de Derecho Procesal*, (53). https://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=423245&d=1

LEGISLACIÓN

Carta de los Derechos Fundamentales de la Unión Europea.

Código Civil Español.

Constitución española de 1978.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, la Intimidad Personal y Familiar y a la Propia Imagen

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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).

Tratado de la Unión Europea.

Tratado de Funcionamiento de la Unión Europea.

JURISPRUDENCIA

Sentencia Audiencia Provincial de Valencia 88/2013, de 12 de marzo (FJ:3)

Sentencia del Tribunal Constitucional 7/1994, de 17 de enero (FJ:2)

Sentencia del Tribunal Constitucional 190/1996, de 25 de noviembre (FJ:2)

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre (FJ:2 y 6)

Sentencia del Tribunal Constitucional 14/2003, de 28 de enero (FJ:4)

Sentencia del Tribunal Europeo de Derechos Humanos 14967/89, de 19 de febrero de 1998

Sentencia del Tribunal Supremo 3212/2022 (Sala de lo Civil), de 28 de julio (FJ:3.6)

Sentencia del Tribunal Supremo 724/2023 (Sala de lo Civil), de 7 de febrero

RESOLUCIONES AEPD

Agencia Española de Protección de Datos. Expediente nº PS/00158/2022. https://www.aepd.es/es/documento/ps-00158-2022.pdf

Agencia Española de Protección de Datos. Procedimiento nº PS/00206/2019. https://www.aepd.es/es/documento/ps-00206-2019.pdf

Agencia Española de Protección de Datos. Recurso de Reposición nº RR/00774/2019. https://www.aepd.es/es/documento/reposicion-ps-00206-2019.pdf

Agencia Española de Protección de Datos. Expediente nº EXP202204806. https://www.aepd.es/es/documento/ai-00173-2022.pdf

Agencia Española de Protección de Datos. Recurso de Reposición nº RR/00440/2019. https://www.aepd.es/es/documento/reposicion-td-00114-2019.pdf

Agencia Española de Protección de Datos. Recurso de Reposición Nº RR/00440/2019. https://www.aepd.es/es/documento/reposicion-td-00114-2019.pdf

Agencia Española de Protección de Datos. Expediente nº EXP202209442. Recurso de Reposición https://www.aepd.es/es/documento/reposicion-ps-00492-2022.pdf

ANEXO I

Artículo séptimo LOPDH

"Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.
2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.
3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.
5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.
6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.
8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas."

ANEXO II

Artículo 57 RGPD

"1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de

reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control."

ANEXO II

Artículo 58 RGPD

"1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.”