



**Universitat Autònoma  
de Barcelona**

**EL REGLAMENTO DE PROTECCIÓN DE  
DATOS:**

**ANÁLISIS DE SUS PRINCIPALES NOVEDADES**

Autor: Górriz Mellado, Isaac

Directora del Trabajo: Montserrat Pi Llorens

Trabajo de Final de Grado

Cuarto curso del Grado de Derecho

Facultad de Derecho de la Universidad Autònoma de Barcelona

## **Resumen**

Los datos de las personas han sido normativamente protegidos desde hace décadas. Aun así, en la actualidad esta cuestión ha adquirido una gran relevancia, en especial debido a la cantidad de información personal que es compartida a día de hoy en internet.

En efecto, la tecnología ha provocado una mayor globalización y actualmente los datos personales son utilizados no solo desde un punto de vista social, sino también para fines públicos y privados, con todos los peligros que puede conllevar en cuanto a una posible transferencia de datos indeseada. Ello ha suscitado multitud de conflictos, a los que se ha intentado hacer frente con la normativa vigente a cada momento.

Con el fin de establecer una normativa a la altura de los retos planteados, la Unión Europea adoptó el Reglamento 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.

Este trabajo pretende realizar un estudio sobre el mencionado Reglamento, sus motivaciones, el nivel de protección que ofrece, sus riesgos, sus ventajas, sus novedades, todo ello con el objeto de averiguar si es adecuado para conseguir sus ambiciosos objetivos.

## Índice

Abreviaturas.....	4
Introducción.....	5
I. Breve exposición histórica sobre la protección de datos en el ámbito internacional.....	9
II. El derecho a la protección de datos en la Unión Europea.....	13
A. Los antecedentes de la actual regulación.....	13
A.1. El convenio Europeo de Derechos Humanos.....	13
A.2. El Convenio 108 sobre protección de datos de carácter personal.....	14
A.3. Directiva 95/46/CE.....	17
B. Régimen jurídico actualmente vigente de la protección de datos en la UE.....	20
B.1. Tratado de Lisboa.....	20
B.2. La Carta de los Derechos Fundamentales de la UE.....	21
B.3. Tratado de Funcionamiento de la Unión Europea y Tratado de la Unión Europea.....	22
B.4. El Reglamento 2016/679.....	23
III. Análisis general del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.....	25
A. Origen del Reglamento.....	25
B. Definición actual de la protección de datos a partir del Reglamento...	27

C. Objeto del Reglamento.....	28
D. Ámbito de aplicación.....	29
IV. Principales claves del Reglamento.....	33
A. El consentimiento.....	33
B. Los derechos del interesado.....	36
C. El Delegado de Protección de Datos.....	41
D. Las autoridades de control.....	43
E. El ámbito de la responsabilidad.....	44
V. Análisis de la jurisprudencia de interés.....	47
A. Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, asunto C-131/12.....	48
B. Sentencia del Tribunal de Justicia (Sala Segunda) de 9 de marzo de 2017, asunto C-398/15.....	49
VI. Conclusiones.....	52
VII. Bibliografía.....	60
A. Legislación.....	60
B. Jurisprudencia.....	62
C. Publicaciones.....	63

## **Abreviaturas**

**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 y por el que se deroga la Directiva 95/46/CE.

**DIRECTIVA:** DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

**TFUE:** Tratado de Funcionamiento de la Unión Europea.

**TUE:** Tratado de la Unión Europea.

**TJUE:** Tribunal de Justicia de la Unión Europea.

**STJUE:** Sentencia del Tribunal de Justicia de la Unión Europea.

**AEPD:** Agencia Española de Protección de Datos.

**AN:** Audiencia Nacional

## Introducción

En la sociedad actual, internet se ha convertido en mucho más que una simple red informática mundial, es el medio utilizado por la mayor parte de la población como herramienta social, para realizar operaciones económicas tales como compras y ventas, contratación de servicios, acceso a cuentas bancarias, búsqueda de empleo, e incluso llevar a cabo gestiones frente a una administración pública como la solicitud de una licencia de obras.

A raíz de ello, se ha considerado necesaria la protección de estos datos personales, los cuales en un ámbito tan peligroso como internet han sido utilizados de manera fraudulenta, causando importantes perjuicios en los últimos años, veremos a lo largo de este estudio ejemplos jurisprudenciales.

Como muestra de la preocupación que suscita este asunto, cabe citar una encuesta realizada por la Unión Europea, el “*Special Eurobarometer 431 “Data protection”*”<sup>1</sup> el cual estimaba que el 67% de los europeos encuestados mostraban su preocupación por no tener un control completo sobre la información que facilitaban de forma online.

Si bien la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,<sup>2</sup> fue el primer texto normativo de la Unión Europea que mostró cierta preocupación expresa por el amparo de este derecho, pero se demostró insuficiente con el paso de los años y ello llevó a que la Unión Europea estableciera nuevas normativas.

---

<sup>1</sup> European Commission, “Special Eurobarometer 431 Data protection”, (2015), disponible en: [https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs\\_431\\_en.pdf](https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf), visitado el 28-12-2018.

<sup>2</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050.

Entre ellas, debemos hacer especial referencia al Reglamento General de Protección de Datos 2016/769,<sup>3</sup> en adelante abreviado como RGPD, el cual apareció después de años en los que existía cierta incertidumbre sobre el camino que seguiría la Unión Europea frente a las necesidades de una sociedad que precisaba una actualización normativa respecto a la protección de datos. Cabe destacar que la forma utilizada ha sido la del Reglamento, con todo lo que ello implica a nivel de uniformidad y aplicabilidad directa y obligatoria, a la que alude el mismo Reglamento en su artículo 99.

Dicha norma subraya en su exposición de motivos que desde el fenómeno de integración realizado por la Unión Europea tienen lugar una gran cantidad de intercambios de datos personales entre Estados Miembros y también entre estos y otros países que no forman parte de la Unión. Pero hoy en día, como consecuencia de los avances tecnológicos, de la globalización y de la gran importancia que presentan los datos personales para los entes tanto públicos como privados, el número de datos intercambiados es exponencialmente superior. En efecto, las personas físicas propagan una considerable cantidad de información personal, de la que se benefician tanto las empresas privadas como las autoridades públicas, puesto que para ambos la obtención de esa información es más fácil de lo que nunca había sido.

Ello ha implicado en los últimos años una mayor sensación de inseguridad e incluso temor por el uso que pueda darse a los detalles personales de cada individuo, lo cual ha llevado a los Estados de todo el mundo a tener que revisar sus normativas y en caso necesario actualizarlas, tal y como ha sucedido en el ámbito comunitario con la implantación del nuevo Reglamento 2016/679, que deroga la anterior Directiva 95/46/CE.

---

<sup>3</sup> 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). OJ L 119, 4.5.2016, p. 1–88.

La Doctora Gemma Minero Alejandre,<sup>4</sup> afirma que actualmente la efectiva protección de datos personales es mucho más compleja que en años anteriores:

*“Antaño, el paso del tiempo se llevaba consigo la información de una persona, a salvo de los residuos que pudieran permanecer en la memoria de quienes conocieron los datos de ésta. Sin embargo, a día de hoy Internet permite rastrear y almacenar de manera fácil información sobre cualquier sujeto, que quedará a disposición del resto de internautas en el futuro, sin que el transcurso del tiempo implique su pérdida”.*

En el mismo estudio, se hace referencia también a lo que supone para los entes privados:

*“Los datos personales se han convertido en un activo importante para numerosas empresas dedicadas al uso, recogida, agregación y análisis de datos de clientes potenciales, que pretenden la monitorización de la conducta de los usuarios de Internet, teniendo como principal exponente el empleo generalizado de cookies”.*

En este mismo sentido, otros autores<sup>5</sup> destacan también los peligros del internet de las cosas, que se encuentran a modo de ejemplo en las aplicaciones móviles, capaces de recabar desde datos de la salud personal hasta el consumo de luz, generándose información muy útil para las empresas.

---

<sup>4</sup> MINERO ALEJANDRE, Gemma, “Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea”, *Anuario Jurídico y Económico Escorialense*, N° 50, (2017), p.15, disponible en: <https://dialnet.unirioja.es/descarga/articulo/5876163.pdf>, visitado el 20-11-2018.

<sup>5</sup> PANIZA FULLANA, Antonia, “Una nueva era en la privacidad y las comunicaciones electrónicas: la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas”, *Revista Doctrinal Aranzadi Civil-Mercantil*, N° 7, (2017), p. 1.



En base a lo expuesto, cabe concluir que la situación actual de la protección de datos es una cuestión de gran interés, puesto que se están produciendo constantes cambios en todo lo concerniente a su trato, influencia, y transmisión, es que conlleva la aparición de peligros anteriormente inexistentes o frecuentes en menor medida, frente a los cuales deberán preverse normativas a la altura.

Este trabajo tiene como objetivo principal el estudio de la protección de datos en el ámbito de la Unión Europea, teniendo en cuenta de manera especial el nuevo RGPD, dado el impacto que ha supuesto para los estados miembros. A fin de poder conseguir este objetivo principal, se desarrollarán otros objetivos secundarios: el primero de ellos será averiguar que se entiende en el ámbito europeo por protección de datos, cuánto abarca y su regulación actual; posteriormente cabrá investigar la regulación vigente en Europa antes del citado Reglamento, los motivos que llevaron a su derogación y un análisis sobre las mismas; en tercer lugar analizar la jurisprudencia llevada a cabo por tribunales de la Unión Europea en materia de protección de datos, estudiando así como se entiende el derecho desde un punto de vista jurisprudencial; y por último averiguar si a raíz del estudio realizado puede observarse una normativa a la altura de los presentes riesgos en relación a la protección de datos.

## I. Breve exposición histórica sobre la protección de datos en el ámbito internacional

Aunque se trata de un derecho considerablemente reciente, las raíces de la protección de datos personales se encuentran en los Estados Unidos de finales del siglo XIX, con la protección a la esfera privada desarrollada por Warren y Brandeis,<sup>6</sup> quienes en su obra *“The Right to Privacy”*<sup>7</sup> establecieron las bases del derecho a la “privacy”, entendida en un contexto más europeo como intimidad. El enfoque que dicho escrito doctrinal presentaba debe ser tenido en cuenta en la actualidad para obtener una completa comprensión del derecho a la protección de datos, puesto que defendía la facultad de establecer límites entre la vida privada de las personas y la intromisión en ella por parte de terceros. Todo ello con especial mención a los medios de comunicación amarillistas, cuyo auge resultó personalmente molesto para ambos juristas y les motivó a elaborar esta importante obra, fuertemente inspirada en las ideas de Thomas M. Cooley, juez de la Corte Suprema de Michigan y autor de *“A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract”*.<sup>8</sup>

Esta última obra estableció las bases para que el derecho a no ser molestado fuera paulatinamente evolucionando en la actual “privacy”, siendo una de las primeras ocasiones en la historia en que se aludía a la posibilidad de que la intimidad alcanzara protección jurisdiccional.

Partiendo de tales premisas, el derecho a la intimidad y la “privacy” prosiguieron su desarrollo, siendo prueba de ello la Declaración Universal de

---

<sup>6</sup> SALDAÑA DÍAZ, María Nieves, “El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego”, *Teoría y Realidad Constitucional*, N° 28, (2011), p. 280, disponible en: [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjfk\\_HjjObfAhXFRBUIHTXPCvgQFjABegQICBAB&url=https%3A%2F%2Fdialnet.uniri](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjfk_HjjObfAhXFRBUIHTXPCvgQFjABegQICBAB&url=https%3A%2F%2Fdialnet.uniri)

[ria.es%2Fservlet%2Farticulo%3Fcodigo%3D3883001&usg=AOvVaw2z9cyfK5naWdDCFrncPefe](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjfk_HjjObfAhXFRBUIHTXPCvgQFjABegQICBAB&url=https%3A%2F%2Fdialnet.uniri) visitado el 23-11-2018.

<sup>7</sup> WARREN, S., & BRANDEIS, L., *“The Right to Privacy”*, Harvard Law Review, vol. 4 N° 5, (1890), pp.193-220, disponible en [https://www.jstor.org/stable/1321160?seq=1#metadata\\_info\\_tab\\_contents](https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents), visitado el 08-01-2019.

<sup>8</sup> COOLEY MCINTYRE, Thomas, *“A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract”* Callaghan, (1879).

Derechos Humanos,<sup>9</sup> que ofrece en el doceavo de sus artículos una protección que abarca parte importante de los derechos de la persona frente a la intromisión de terceros: “*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*”. La progresiva transformación del derecho a la intimidad ocasionó un nuevo derecho forjado especialmente a partir de 1970 referente a la protección de datos personales<sup>10</sup> en una vertiente más similar a la existente hoy en día, aunque el primer pronunciamiento de la Tribunal Europeo de Justicia referente al conflicto entre la intimidad y la protección de datos tuvo lugar con un poco de anterioridad.<sup>11</sup>

Cabe de nuevo reafirmar el liderazgo de Europa en el presente ámbito. Corría el año 1967 cuando el Consejo de Europa estableció una Comisión consultiva para evaluar las posibles vulneraciones que podían presentar las nuevas tecnologías frente a los derechos de las personas. El resultado de ello fue la Resolución 509 de 1968 de la Asamblea del Consejo de Europa que constataba la ya evidente peligrosidad de tales avances en la vida de las personas.

En dicho contexto, los Estados no tardarían en establecer legislaciones que trataran de amparar tales peligros, siendo Alemania la pionera<sup>12</sup> al promulgar en 1970 una ley de protección de datos moderna.<sup>13</sup>

Poco después le seguirían otros países como Suecia con su Ley de Protección de Datos de mayo de 1973; Estados Unidos con el Privacy Act de 1974,

---

<sup>9</sup> ONU Asamblea General, Declaración Universal de Derechos Humanos, 10 diciembre 1948, disponible en: <http://www.un.org/es/universal-declaration-human-rights/>, visitado el 01-03-2019.

<sup>10</sup> BALDUCCI ROMANO, Fabio, “The Right to the Protection of Personal Data: A New Fundamental Right of the European Union”, *SSRN Electronic Journal*, (2013), p. 1, disponible en SSRN: <https://ssrn.com/abstract=2330307>, visitado el 20-11-2018.

<sup>11</sup> Sentencia del Tribunal de Justicia de 12 de noviembre de 1969. Erich Stauder contra Stadt Ulm - Sozialamt. Asunto 29-69. ECLI:EU:C:1969:57, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A61969CJ0029>, visitado el 13-03-2019.

<sup>12</sup> BANISAR, David and DAVIES, Simon G., “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments”, *John Marshall Journal of Computer & Information Law*, Vol. XVIII, (2012), p. 10, disponible en <https://ssrn.com/abstract=2138799>, visitado el 13-03-2019.

<sup>13</sup> Hessisches Datenschutzgesetz, de 7 de octubre de 1970, disponible en [https://www.rv.hessenrecht.hessen.de/lexsoft/default/hessenrecht\\_rv.html#docid:8074311,2,20180525](https://www.rv.hessenrecht.hessen.de/lexsoft/default/hessenrecht_rv.html#docid:8074311,2,20180525)

considerado “auténtico precursor de las posteriores normas sobre protección de datos de carácter personal”;<sup>14</sup> o Francia a través de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Paralelamente, en el año 1973 una nueva Resolución del Consejo de Europa<sup>15</sup> invitaba a los Estados a actualizar sus legislaciones en aras de proteger los derechos personales frente a las injerencias que podían suponer los usos fraudulentos de datos de índole personal por bancos de datos en el sector privado. Posteriormente, se emitió una Resolución referente al mismo objeto, pero esta vez centrada en el ámbito público.<sup>16</sup> De este modo proseguía la concienciación colectiva aunque fuere en sectores determinados, hecho que cambiaría considerablemente a partir de la elaboración de uno de los documentos que más inspirarían a las normativas venideras referentes a la materia,<sup>17</sup> el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.<sup>18</sup> Dicho Convenio aumentaba transfronterizamente las garantías dedicadas a la protección de los datos personales, instaurando a modo de ejemplo autoridades independientes que se encargaran de velar por el cumplimiento de la norma. Las insuficiencias de este último Convenio serían suplidas por la Directiva 95/46/CE, que será tratada en varias ocasiones a lo largo del presente trabajo y supone uno de los más importantes avances legislativos en la historia de la protección de datos por razones que serán expuestas con posterioridad.

A partir de este maremágnum de normas, documentos y escritos doctrinales, se formó la actual normativa internacional de protección de datos, que a día de hoy se incluye en el organigrama jurídico de multitud de países, siendo ejemplo de ello la Lei de Protecção de Dados Pessoais a Informática, en 1992, la Ley 25.326 sobre

---

<sup>14</sup> REBOLLO DELGADO, Lucrecio, GÓMEZ SÁNCHEZ, Yolanda, “*Biomedicina y protección de datos*” Dykinson, (2008) p. 23.

<sup>15</sup> Resolución 73/22 del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, durante la 224ª reunión de los Delegados de los Ministros, adoptada el 26 de septiembre de 1973.

<sup>16</sup> Resolución 74/29 del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974, durante la 236ª reunión de los Delegados de los Ministros

<sup>17</sup> BANISAR y DAVIES, *op. cit.*, p. 10.

<sup>18</sup> Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ETS n.º 108, 28-1-1981.

Protección de los Datos Personales en Argentina, o el Acuerdo Marco de Protección de Datos entre la UE y los EE.UU.

## **II. El derecho a la protección de datos en la Unión Europea**

El presente apartado se destina a estudiar tanto desde un punto de vista histórico como actual el desarrollo de la protección de datos en el ámbito europeo.

### **II.A. Los antecedentes de la actual regulación**

Se analizará en este punto la normativa que paulatinamente fue forjando el derecho a la protección de datos.

#### **II.A.1. El convenio Europeo de Derechos Humanos**

En primer lugar, cabe hacer referencia al Convenio Europeo de Derechos Humanos,<sup>19</sup> firmado en 1950 por el Consejo de Europa bajo la estela de la Declaración Universal de Derechos Humanos de 1948, de la que se influyó notablemente.

Pese a ser un tratado internacional, su carácter protector de los derechos humanos y las libertades fundamentales en Europa lo hacen especialmente relevante para el estudio de la introducción paulatina del derecho a la protección de datos en Europa. En este sentido, el Convenio reconoce en el octavo de sus artículos el derecho a la vida privada, del que posteriormente se derivaría el derecho a la protección de datos: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”.

Naturalmente, este derecho no era absoluto, pudiendo ser limitado en virtud de la ley, la seguridad nacional o pública, la economía, la defensa, las infracciones penales, la salud, la moral o los derechos y libertades de los demás.

La inclusión del derecho a la vida privada en el Convenio fue relevante en primer lugar porque a partir de este precepto se desarrollaría el derecho a la

---

<sup>19</sup> Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, ratificado por España el 26 de septiembre de 1979. Boletín Oficial del Estado núm. 243/1979, de 10 de octubre, p. 23564 a 23570.

protección de datos en posteriores regulaciones europeas. Y en segundo término porque permitiría el amparo jurisdiccional del derecho a la protección de datos ante el Tribunal Europeo de Derechos Humanos, creado por el mismo Convenio con el objetivo de proteger a las personas de la violación de los derechos humanos.

Decimos que el Convenio permitió el amparo jurisdiccional de la protección de datos puesto que, aunque el CEDH no reconocía expresamente este derecho, el TEDH lo entendió comprendido dentro del artículo dedicado a la protección de la vida privada.

De este modo, el papel del TEDH ha sido fundamental en el ámbito de la protección de datos atendiendo a que la indefinición del artículo 8 del CEDH ha permitido que el Tribunal estableciera el amparo de multitud de derechos que ha entendido incluidos en el precepto, entre ellos la protección de datos: *“así lo ha entendido el TEDH con una doctrina en que la vaguedad conceptual se ha puesto, en buena medida, al servicio de una interpretación generosa y extensiva de tal derecho, dando lugar a que a través del mismo se haya dado protección a situaciones referidas a temas tan diversos como, por ejemplo, la identidad sexual, la protección de datos personales, las relaciones paterno-filiales o las cuestiones medio-ambientales”*.<sup>20</sup>

## **II.A.2. El Convenio 108 sobre protección de datos de carácter personal**

A partir de la década de los 60, el Consejo de Europa aumentó su preocupación por los derechos relacionados con la vida privada,<sup>21</sup> lo que conllevó la adopción de dos Resoluciones en los años 70 ya referidas anteriormente, concernientes a la protección de las personas físicas respecto de los bancos de datos electrónicos en los sectores privado y público.

---

<sup>20</sup> PÉREZ DE LOS COBOS ORIHUEL, Francisco “El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado”, *Unidad Biblioteca de Derecho Comparado, Dirección General de Servicios de Estudios Parlamentarios (DG EPRS) de la Secretaría General del Parlamento Europeo*, (2018), p. 6, [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS\\_STU\(2018\)628261\\_E\\_S.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_E_S.pdf), visitado el 05-04-2019.

<sup>21</sup> PÉREZ DE LOS COBOS *op. cit.*, p.2.

Sendas resoluciones sirvieron como antecedentes del Convenio n° 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que también ha sido mencionado en el presente trabajo, pero será analizado con más profundidad en este apartado.

Aunque el ámbito de aplicación territorial del presente Convenio no se limita a los Estados Miembros del Consejo de Europa, sino que se permite la inclusión de otros países no europeos ostentando un alcance universal, su importancia en la regulación europea conlleva que deba ser estudiado en este apartado.

Tal y como se desprende de sus considerandos, el Convenio tiene el objetivo de ampliar el derecho a la vida privada consagrado en el artículo 8 del CEDH, especialmente a raíz del incremento de la circulación entre países de datos personales tratados automatizadamente. Todo ello sin olvidar el necesario reconocimiento de la libertad de circulación interestatal de la información.

De forma temprana, en el primero de sus artículos ya se incluye el término “protección de datos”, determinando que el fin concreto del Convenio es garantizar a toda persona dentro del territorio de los Estados Parte el derecho a la vida privada frente al tratamiento automatizado de los datos personales, independientemente de su nacionalidad o residencia. Se muestra en este precepto como a pesar de hacer referencia a la protección de la vida privada reconocida en el CEDH se está ampliando el contenido de este derecho al entenderlo vulnerado por el tratamiento indebido de los datos personales.

Este “tratamiento automatizado” al que refiere constantemente el Convenio se define como una serie de operaciones llevadas a cabo con ayuda de procedimientos automatizados, concretamente el registro de datos, la aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión. Se trata pues de un concepto que pese al momento en el que fue elaborado abarca un conjunto de operaciones a tener en cuenta.



Aunque las Partes se comprometen a aplicar el presente Convenio al tratamiento automatizado de datos tanto en el sector público como privado, las garantías que ofrecía el Convenio no dejaban de ser mínimas. Además, los Estados contaban con una considerable flexibilidad al permitírseles que no aplicaran el Convenio a determinadas categorías de ficheros de datos de carácter personal a su elección, tal y como se establece en el apartado segundo, letra “a” del artículo 3:

*“Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior hacer saber mediante declaración dirigida al Secretario general del Consejo de Europa: Que no aplicará el presente Convenio a determinadas categorías de ficheros automáticos de datos de carácter personal, una lista de las cuales quedará depositada”.*

Tal flexibilidad se extiende también al cumplimiento de una serie de principios básicos para la protección de datos, que aluden a la calidad de estos, su lícita recogida, su confidencialidad y el establecimiento de medidas de seguridad, todo ello para ofrecer las garantías necesarias a las personas implicadas.

En base a dichos principios los Estados debían tomar en su derecho interno las medidas necesarias para hacerlos efectivos, no obstante, tal obligación fue incumplida por países como España, *“nuestro país ha venido incumpliendo algunas de las obligaciones jurídico-internacionales establecidas en su texto normativo, referidas precisamente a la elaboración y aprobación de la mencionada legislación interna y explicitadas en el art. 4 del Convenio”*.<sup>22</sup>

Asimismo, se prevén ciertas excepciones en las que se permite el incumplimiento de los mencionados principios, algunas de carácter público consistentes en la seguridad estatal, los intereses monetarios del Estado o la

---

<sup>22</sup>PAVÓN PÉREZ, Juan Antonio, “La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales”, *Anuario de la Facultad de Derecho*, N° 19, (2001), p. 239, disponible en <https://dialnet.unirioja.es/descarga/articulo/831270.pdf>, visitado el 16-04-19.

represión de infracciones penales; y otras de índole privada como la protección de la persona y de los derechos y libertades de otras personas.

A tenor del artículo 10 del Convenio, las sanciones previstas en caso de vulnerar tales principios serán las que establezca cada Parte, sin mayor especificación.

Cabe aclarar que en lo referente a las transferencias de datos solo se regulan aquellas llevadas a cabo entre los Estados Parte prevaleciendo de forma casi absoluta la libre circulación de estos.

En conclusión, si bien el Convenio es jurídicamente vinculante para los Estados Parte, contiene numerosas excepciones que sumadas a una regulación falta de exigencias reales y efectivas facilitaron su incumplimiento. Aun así, ostenta cierto valor al ser el primer texto internacional jurídicamente vinculante concerniente al derecho de protección de datos, introducir conceptos que serían desarrollados en posteriores normativas, y servir como antesala de la Directiva 95/46/CE.

### **II.A.3. Directiva 95/46/CE**

El derecho a la protección de datos se estableció estrictamente por primera vez en la Unión Europea con la Directiva 95/46/EC,<sup>23</sup> tomando las siguientes como bases jurídicas: en primer lugar, el ya referido Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

En segundo término, el artículo 7 A del Tratado Constitutivo de la Comunidad Europea en su versión modificada por el Tratado de Maastrich en 1992. Ello se reconoce en el tercero de los considerandos de la Directiva, que alude a que dentro de la libre circulación de mercancías, personas, servicios y capitales, es necesaria la libre circulación de datos y por ende debe garantizarse la protección de los mismos.

---

<sup>23</sup> BALDUCCI, *op. cit.*, p. 1.

Y por último el anteriormente mencionado Convenio 108, cuyos principios deberá ampliar considerablemente en aras de perseguir una protección del derecho adecuada a su tiempo.

En 1990, la Comisión Europea llevó a cabo la primera propuesta de la Directiva, naturalmente Internet no se concebía entonces como un elemento tan influyente en la sociedad, siendo utilizando en menor medida y con fines distintos, por tanto, esta norma debe ser analizada bajo el prisma de la época en que fue realizada.

En este sentido, cabe destacar el artículo primero de la Directiva, donde queda patente que aún se entendía la protección de datos como un derecho necesariamente ligado a la intimidad, alejándose de la percepción actual en la que consideramos que es un derecho autónomo y diferenciado, tal y como muestra el RGPD también en el artículo número uno. Posteriormente, en el apartado segundo del mismo precepto, encontramos uno de los puntos que más controversia causaron, ya que se establece lo siguiente: *“Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1”*, es decir, aunque se prevé una protección a este derecho, la libre circulación de los datos personales está por encima, o dicho con otras palabras, *“la Directiva no debe ser entendida como un sistema de protección de las personas sino como un intento de impedir las trabas a la libre circulación de la información personal en el ámbito comunitario”*.<sup>24</sup>

En el artículo segundo, se recoge la definición de datos personales, basándose en el amplio reconocimiento de *“toda información sobre una persona física identificada o identificable”*; Por otra parte, en lo que concierne a la

---

<sup>24</sup> HERRÁN ORTIZ, Ana Isabel, *“El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales”*, Dykinson, p. 2, (2003), extracto disponible en: <http://vlex.com/vid/directiva-frente-libre-circulacion-190765>, visitado el 11-12-2018.

definición de consentimiento del interesado, no se exigía que este fuera inequívoco ni que tuviera que darse mediante una declaración o una clara acción afirmativa.

Respecto al ámbito de aplicación, se excluía en virtud del artículo 3 el tratamiento de datos realizado por motivos de seguridad pública, defensa, seguridad del Estado, o actividades estatales conectadas con el Derecho Penal, ya sean los obtenidos por sonido, imagen o por videocámaras.<sup>25</sup> Tal exclusión está relacionada con el reparto de competencias de la UE, dado que las actividades mencionadas no estaban comprendidas en el ámbito de aplicación del Derecho comunitario a tenor de los títulos V y VI del TUE.

Por su parte, la aplicación territorial era en gran medida limitada, atendiendo a que el establecimiento responsable de realizar el tratamiento ilícito debía encontrarse en el territorio de un Estado Miembro, con lo cual, cualquier empresa que tratara datos personales de un ciudadano de la Unión desde fuera del ámbito comunitario no quedaba sujeta a la Directiva.

Otro punto importante de la Directiva era la obligación de los Estados Miembros a asegurarse que *“toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate”*. Este artículo 22, por lo tanto, salvaguarda los datos personales de cualquier injerencia indeseada dando la posibilidad a toda persona de hacer valer su derecho frente a los tribunales que cada Estado Miembro considere adecuados.

Al tratarse de una Directiva, otorgaba cierta libertad a los Estados, al facultarles de forma limitada para establecer las condiciones en que es lícito el tratamiento de datos, elemento que podía provocar una aplicación diferenciada según las condiciones especiales adoptadas por cada Estado. También se dejaba al arbitrio de los Estados la determinación de las sanciones provocadas por el incumplimiento de esta norma comunitaria.

---

<sup>25</sup> HERRÁN, *op. cit.*, p. 7.

El mismo Balducci Romano, autor del estudio anteriormente aludido,<sup>26</sup> señala como principal objetivo de la Directiva la necesidad comunitaria de eliminar los obstáculos que impedían la libre circulación de datos personales, lo cual sería ampliamente beneficioso para el mercado común, “*The Directive’s aim is to remove the obstacles to the free movement of personal data, necessary to complete the full establishment of the internal market*”. Todo ello bajo el aura de protección a los derechos humanos que debe tener en cuenta cualquier normativa europea.

Definitivamente, en ciertos aspectos tal Directiva no se distancia en gran medida del Reglamento que se encargó de sustituirla. Ello es reconocido expresamente en el Considerando noveno de dicho RGPD, el cual establece que siguen siendo válidos los valores y principios enumerados en la Directiva. Aun así, el mismo considerando pone de manifiesto que la forma jurídica que la revistía provocaba una aplicación diferenciada en los Estados Miembros a causa de su necesaria transposición, lo cual conllevaba inseguridad jurídica y dificultad en la transmisión de dichos datos por la Unión, siendo este uno de los mayores detonantes de su derogación. Además, el plazo fijado para dicha transposición fue de 12 años, hecho que provocó una adaptación tardía de la directiva en algunos países.<sup>27</sup>

## **II.B. Régimen jurídico actualmente vigente de la protección de datos en la UE**

A continuación, se hará referencia a la normativa que hoy en día regula la protección de datos de carácter personal en la Unión Europea.

### **II.B.1. Tratado de Lisboa**

La entrada en vigor del Tratado de Lisboa<sup>28</sup> el 1 de diciembre de 2009 supuso el establecimiento de una nueva base jurídica para el derecho a la protección

---

<sup>26</sup> BALDUCCI, *op. cit.*, p. 3.

<sup>27</sup> European Commission, “First report on the implementation of the Data Protection Directive, (2003), disponible en <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:HTML>, visitado el 11-12-2018.

<sup>28</sup> Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, OJ C 306, 17.12.2007, p. 1–271, disponible en [http://www.europarl.europa.eu/ftu/pdf/es/FTU\\_1.1.5.pdf](http://www.europarl.europa.eu/ftu/pdf/es/FTU_1.1.5.pdf)

de datos al introducir el artículo 16 del nuevo Tratado de Funcionamiento de la Unión Europea: *“Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen”*. Además, convirtió este derecho en fundamental al atribuir a la Carta de los Derechos Fundamentales de la UE el carácter de jurídicamente vinculante.

Tanto la base jurídica establecida en el TFUE como el nuevo valor de la Carta serán analizados de forma más específica a continuación, interesando en el presente apartado únicamente hacer una breve referencia a los mismos en tanto a que fueron implementados por el Tratado de Lisboa.

Este Tratado de modificación también fue el encargado de formalizar la adhesión de la UE al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, garantizando que los derechos previstos en él formarán parte del Derecho de la Unión como principios generales.

## **II.B.2. La Carta de los Derechos Fundamentales de la UE**

Aprobada en el año 2000 con el objetivo de instaurar un conjunto de derechos, libertades y principios entendidos como necesarios para el progreso de la sociedad, y de los avances tecnológicos y científicos, la Carta de los Derechos Fundamentales de la Unión Europea<sup>29</sup> no tomó valor vinculante hasta la aprobación del Tratado de Lisboa, momento en el que fue revestida de una mayor importancia. Por esta razón es analizada en el presente estudio en un orden posterior a dicho Tratado.

Aunque la Carta no forme parte del Tratado de Lisboa, este tratado modificativo le otorgó valor jurídico vinculante al introducir en el artículo 6 del nuevo Tratado de la Unión Europea el siguiente redactado:

*“La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de*

---

<sup>29</sup> Carta de los Derechos Fundamentales de la Unión Europea, OJ C 326, 26.10.2012, p. 391–407, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012P/TXT&from=ES>

2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados”.

En este sentido, la consideración de la protección de datos como derecho fundamental se recoge en el artículo 8 de la Carta, de forma inmediatamente posterior al respeto a la vida privada y familiar, siendo entendidos por tanto como dos derechos autónomos y diferenciados el uno del otro. El reconocimiento de la protección de datos en el octavo de sus artículos, incluido dentro del capítulo II concerniente a las libertades es muestra de la importancia que se le otorga a tal derecho.

El citado precepto se divide en tres apartados: el primero de ellos atribuye a toda persona el derecho a la protección de sus datos personales; el segundo se enfoca en el tratamiento, que deberá ser leal, para fines concretos y basado en el consentimiento u otro fundamento legítimo. Asimismo, concede a toda persona tanto el acceso a sus datos como su posterior rectificación; por último, el tercero de los apartados atribuye el control del cumplimiento de estas normas a una autoridad independiente, sin mayor concreción.

Por ende, no se incluye definición alguna referente a qué entiende la Carta por datos personales, consentimiento o tratamiento, remitiéndose así a la normativa comunitaria reguladora de la materia que deberá esclarecer tales conceptos.

### **II.B.3. Tratado de Funcionamiento de la Unión Europea y Tratado de la Unión Europea**

El Tratado de Funcionamiento de la Unión Europea,<sup>30</sup> reconoce también el derecho a la protección de datos personales a “*toda persona*” en su artículo 16.1, tratándose de un precepto calcado al 8.1 de la CDFUE.

---

<sup>30</sup> Tratado de Funcionamiento de la Unión Europea, OJ C 326, 26.10.2012, p. 47–390, disponible en [http://data.europa.eu/eli/treaty/tfeu\\_2012/oj](http://data.europa.eu/eli/treaty/tfeu_2012/oj)

El segundo de sus apartados atribuye al Parlamento europeo y al Consejo el establecimiento de normas sobre la protección de las personas físicas respecto del tratamiento de sus datos por las instituciones, órganos, organismos de la UE, así como por los Estados Miembros cuando ejerzan actividades comprendidas en el ámbito de aplicación del Derecho de la Unión.

Se hace referencia en el segundo apartado de este precepto al control que deberá llevar a cabo una autoridad independiente sobre la debida aplicación de dichas normas, las cuales deberán establecerse con arreglo al procedimiento ordinario.

El artículo 16 finaliza remitiéndose al artículo 39 del Tratado de la Unión Europea,<sup>31</sup> donde se prevé que el Consejo fijará en una decisión *“las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes”*.

Por su parte, el Tratado de la Unión Europea interesa en cuanto al estudio de la protección de datos en los términos ya referidos, atendiendo a que concede a la Carta valor jurídicamente vinculante en su artículo 6 introducido por el Tratado de Lisboa y atribuye al Consejo el deber de fijar en una decisión las normas sobre la materia.

#### **II.B.4. El Reglamento 2016/679**

El RGPD será objeto de un análisis más exhaustivo posteriormente, sin embargo, cabe hacer en el presente apartado una breve referencia al ser parte importantísima del régimen jurídico actual de la protección de datos.

---

<sup>31</sup> Tratado de la Unión Europea, OJ C 326, 26.10.2012, p. 13–390, disponible en [https://eur-lex.europa.eu/eli/treaty/teu\\_2012/oj](https://eur-lex.europa.eu/eli/treaty/teu_2012/oj)



En el primero de sus considerandos hace referencia expresa a la CDFUE y al TFUE reivindicando que la protección de datos es un derecho fundamental reconocido a toda persona tal y como en ellos se señala.

De este modo, como conclusión al presente apartado cabe referir que tras la evolución normativa experimentada es posible afirmar que actualmente en Europa se garantiza el derecho a la protección de datos en términos amplios, ya que tal y como señala Ana Isabel Herrán Ortiz: *“No se limita, sin embargo, el legislador europeo a proclamar dicha consideración, bien al contrario, extiende dicha protección a las personas físicas “cualquiera que sea su nacionalidad o residencia”, vinculando directamente los principios y normas relativos a la protección de las personas físicas en el tratamiento de sus datos personales, con el respeto a las libertades y los derechos fundamentales”*.<sup>32</sup>

---

<sup>32</sup> HERRÁN ORTIZ, Ana Isabel, “Aproximación al derecho a la protección de datos personales en Europa. El reglamento general de protección de datos a debate” *Revista de Derecho, Empresa y Sociedad (REDS)* N° 8, (2016), p.181, disponible en <https://dialnet.unirioja.es/descarga/articulo/6140105.pdf>, visitado el 11-11-2018.

### **III. Análisis general del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE**

#### **III. A. Origen del Reglamento**

En el año 2009, el Parlamento Europeo, en su Resolución sobre el Programa de Estocolmo,<sup>33</sup> dio especial importancia a la necesidad de elaborar una normativa sobre protección de datos que se adaptara a las necesidades actuales, tal y como se establece en el apartado ochenta y tres: *“Insiste en que en todas las políticas de la Unión se garantice el respeto de la dimensión de los derechos fundamentales que tienen la protección de datos y el derecho a la vida privada”*. Ya en 2011, tras un periodo de consultas y reuniones tanto de índole pública como privada, con gobiernos nacionales, ONG’ s, expertos y autoridades de protección de datos,<sup>34</sup> el Parlamento Europeo emitió la resolución de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea<sup>35</sup> en la que entiende que, si bien los principios establecidos en la Directiva 95/46/CE son un punto de partida a tener en cuenta, los desarrollos tecnológicos han conllevado peligros que esta anterior normativa no puede proteger y que por tanto era necesario un nuevo marco legal capaz de garantizar una aplicación uniforme sobre la protección de datos en Europa.

---

<sup>33</sup> Resolución del Parlamento Europeo, de 25 de noviembre de 2009, sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos – Programa de Estocolmo", disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2009-0090+0+DOC+PDF+V0//ES>

<sup>34</sup> KUNER, Christopher, “The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law”, *Bloomberg BNA Privacy and Security Law Report*, (2012), pp. 1-15, disponible en [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2162781](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781), visitado el 22-11-2018.

<sup>35</sup> Resolución del Parlamento Europeo, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI)), disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES>, visitado el 15-1-2019.

Dado el cierto consenso existente, la Comisión Europea decidió en 2012 llevar a cabo una primera Propuesta<sup>36</sup> sobre lo que finalmente sería el RGPD, el cual sufriría diversas modificaciones al largo de los años posteriores. Se trataba no solamente de una preocupación institucional, sino que también estaba instaurada en la ciudadanía de la Unión, cuya inquietud por la utilización fraudulenta de sus datos era considerable.<sup>37</sup>

Aun así, no se trató de una regulación fácil de aprobar, de hecho, fue una de las más complicadas que tuvo que afrontar la Unión, *“la dificultad para llegar a un texto de consenso se evidenció por el hecho de ser la propuesta legislativa que ha recibido mayor número de enmiendas, más de 3.000, en toda la historia del Parlamento. No fue hasta diciembre de 2015, ya con las nuevas instituciones surgidas tras las elecciones de 2014, cuando se alcanzó el acuerdo”*.<sup>38</sup>

Finalmente, Parlamento y Consejo llegaron a un acuerdo sobre el texto final y este sería publicado en el Diario Oficial de la Unión Europea a 4 de mayo de 2016, entrando en vigor el día 24 del mismo mes. Aun así, su aplicación no sería preceptiva hasta el 25 de mayo, pero del año 2018, otorgando tiempo tanto a los Estados Miembros como a las empresas para adaptarse a las nuevas exigencias.

---

<sup>36</sup> Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos) Bruselas, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), disponible en: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF>

<sup>37</sup> European Commission, Special Eurobarometer 431 “Data protection”, (2015), p. 115, disponible en: [https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs\\_431\\_en.pdf](https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf), visitado el 12-12-2018.

<sup>38</sup> GÓMEZ BARROSO, José Luís; FEIJÓO, Claudio; MARTÍNEZ, Dolores F.; “Política antes que regulación: la protección de la información personal en la era del big data”, *Economía industrial*, N.º. 405, (2017), p. 116, disponible en: <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/GÓMEZ,%20FEIJOO%20Y%20F.%20MARTÍNEZ.pdf>, visitado el 12-12-2018.

### III.B. Definición actual de la protección de datos a partir del Reglamento

Podemos obtener una definición actual de la protección de datos a partir del concepto que nos brinda el artículo 4. 1 del RGPD:

*“**Toda información** sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”*

A partir de este precepto, obtenemos que se trata de una protección con un amplio objeto, ya que se ampara toda información de las personas físicas vivas y que se encuentren dentro del ámbito de aplicación del Reglamento.

La Unión Europea ha llevado a cabo tareas de definición de los datos personales previamente, como el *“Dictamen 4/2007 sobre el concepto de datos personales”*,<sup>39</sup> donde el grupo de trabajo señala la *“intención del legislador europeo de mantener un concepto amplio de «datos personales»”*, haciendo también referencia a que, en la propuesta modificada por la Comisión de la Directiva 95/46/CE, se expresaba el *“deseo del Parlamento de que la definición de “datos personales” sea tan amplia como sea posible con el fin de incluir toda información referente a una persona identificable”*. Con un concepto tan extenso, la Unión Europea pretende abarcar la protección de la mayor parte de datos personales posible.

A tenor de ello, el medio empleado para tratar y almacenar estos datos no es relevante para establecer la protección o no de los mismos, tal y como establece la página web de la Unión Europea en su apartado referente a los datos personales *“El RGPD protege los datos personales **independientemente de la tecnología utilizada para su tratamiento** (...) Asimismo, no importa cómo se conservan los datos; ya sea en un sistema informático, a través de videovigilancia*

---

<sup>39</sup> Grupo de protección de las personas en lo que respecta al tratamiento de datos personales del artículo 29, Dictamen no 4/2007 sobre el concepto de datos personales adoptado el 20 de junio de 2007 (WP 136).

*o sobre papel”*.<sup>40</sup>

Bajo estos parámetros, serían considerados como datos personales los mencionados en la citada página web de la Comisión Europea: algunos de ellos han sido amparados desde hace décadas, como el nombre y los apellidos de un individuo, el domicilio, una dirección de correo electrónico que incluya datos de la persona, el número de documento nacional de identidad o datos sanitarios; pero otros son más enfocados a las nuevas tecnologías, estos son los datos de localización, tales como la ubicación de los dispositivos móviles, la dirección IP, las cookies, o la publicidad de los dispositivos móviles como el teléfono. En base a esta definición, quedarían lejos de la defensa del Reglamento los números del Registro Mercantil, las direcciones de correo electrónico que no contengan datos personales y los datos anonimizados.

### **III.C. Objeto del Reglamento**

El objeto del Reglamento, tal y como se establece en el artículo 1 del mismo, es doble: en primer lugar, en aras de defender los derechos fundamentales comunitarios y en especial la protección de datos, comprende la normativa relativa a la protección de los mismos. En otras palabras, el derecho fundamental recogido en el artículo octavo de Carta Europea de los Derechos Fundamentales de la Unión Europea no será el único protegido, sino que cualquier derecho que pueda ser vulnerado por el trato indebido de los datos personales, como la intimidad, quedará amparado.

Por otra parte, muestra también su voluntad de regular la libre circulación de los datos, conteniendo así un aspecto más relacionado con el libre mercado, una importante preocupación de la Unión Europea. En este sentido, las actividades económicas de la Unión pueden realizarse de manera más ágil en comparación con

---

<sup>40</sup> Comisión Europea, ¿Qué son los datos personales?, disponible en [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_es](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es), visitado el 09-12-2018.

la anterior regulación, al contar ahora con una uniformidad legislativa entre Estados Miembros.<sup>41</sup>

Dicho binomio podría conllevar conflictos en lo que concierne a la situación jerárquica de estos dos elementos, pero el apartado tercero del citado artículo otorga prevalencia de la libre circulación de datos personales, atendiendo a que: “*no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*”.

Este precepto cumple también la función de determinar que dicha normativa protege los datos personales de las personas, únicamente las físicas, aspecto que será analizado posteriormente.

### **III.D. Ámbito de aplicación**

De forma previa, cabe puntualizar que, al tomar la forma de Reglamento, la aplicación es más uniforme en el territorio de los Estados de la Unión en comparación con anteriores regulaciones. La materia objeto de regulación es protegida mediante un instrumento de alcance general, obligatoriedad y aplicabilidad directa en cada Estado Miembro.

En este apartado debemos hacer referencia tanto al ámbito material como al territorial.

Sobre el primero de ellos, el artículo segundo del RGPD indica que dicha norma es de aplicación respecto al tratamiento de datos personales, ya sea total o parcial e independientemente de si se tratan datos automatizados o manuales. Es necesario que estos datos puedan ser incluidos en un fichero, ya que de lo contrario quedarían fuera del alcance del RGPD.<sup>42</sup>

---

<sup>41</sup> HERRÁN, *op. cit.*, p. 4.

<sup>42</sup> BARTOLOMÉ MARTÍN, Antonio, “Sobre el ámbito de aplicación material del reglamento general de protección de datos” *Actualidad Jurídica Aranzadi* N° 943, (2018), p. 8, disponible en <https://cms.law/es/ESP/Publication/Bartolome-Martin-sobre-el-ambito-de-aplicacion-material-del-Reglamento-General-de-Proteccion-de-Datos>, visitado el 22-3-2019.

Llegados a este punto, cabe analizar que se entiende por tratamiento. Este concepto aparece definido en el artículo 4 de la siguiente manera: *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no.”* A continuación, este precepto propone una serie de ejemplos de tratamiento como *“la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”*.

Como vemos, la regulación presenta en este punto una clara similitud con la Directiva 95/46/CE, el considerando 15 del RGPD lo justifica expresando que la protección no debe estar sujeta a las técnicas utilizadas para el tratamiento de datos.

Por otra parte, el Reglamento no es aplicable a actividades excluidas del ámbito de aplicación material del Derecho Comunitario, como serían los supuestos relacionados con la seguridad nacional; tampoco a las actuaciones de los Estados Miembros reguladas en el TUE, capítulo II, Título V referentes a la política exterior y seguridad común; ni a las exclusivamente personales; ni al tratamiento que pueden llevar a cabo las autoridades en aras de investigar o enjuiciar, especialmente en casos de seguridad pública, puesto que para ello será de aplicación la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.<sup>43</sup>

En lo que concierne a la aplicación territorial, esta ha sido extendida respecto a normativas anteriores, puesto que, a partir del RGPD se protege el tratamiento de datos independientemente de donde se encuentre el establecimiento de un responsable o de un encargado de la Unión. De este modo, lo relevante no es si el tratamiento se lleva a cabo dentro de la Unión Europea, sino que el elemento que va a conllevar la aplicación del Reglamento y por ende su protección es que los datos tratados pertenezcan a ciudadanos de la Unión.

---

<sup>43</sup> Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo OJ L 119, 4.5.2016, p. 89–131

En este sentido, entendemos por responsable, de acorde con el artículo 4 del RGPD, a *“la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento”*.

Por su parte, la figura del encargado es anexa a la del responsable, debido a que se encarga de tratar los datos por cuenta de este último. Se trata de una persona, física o jurídica que realiza un servicio a favor del responsable correspondiente en tratar datos personales por su cuenta. En esencia, la figura del responsable se diferencia de la del encargado porque decide la finalidad y los usos de la información, mientras que el encargado se limita a cumplir las órdenes de aquel que le ha solicitado sus servicios referentes al tratamiento de datos personales.<sup>44</sup>

También podrán ser objeto de protección aquellos datos que no sean tratados por establecimientos dentro de la Unión, pero realicen actividades como la oferta de bienes, servicios o su control en la UE, siempre y cuando los interesados a recibir el amparo que ofrece el RGPD residan en la Unión. Incluso se permite la aplicación de este Reglamento cuando el Derecho de los Estados Miembros sea de aplicación en base al Derecho Internacional Público, aunque el responsable no tenga su establecimiento en la UE.

En conclusión, la protección de datos de los ciudadanos de la Unión se ha visto claramente ampliada siendo ahora posible su amparo frente a sociedades encargadas de tratar con datos de europeos desde un país externo, tal y como afirma Mayor Gómez: *“el RGPD resulta también de aplicación al tratamiento de datos fuera de la Unión Europea, lo que amplía de forma considerable su ámbito de aplicación ya que permitirá, por ejemplo, que sea aplicable a empresas que, hasta este momento, podían estar tratando datos de personas en la Unión Europea y que,*

---

<sup>44</sup> Autoritat Catalana de Protecció de Dades en col·laboració amb l'Agència Espanyola de Protecció de Dades i l'Agència Basca de Protecció de Dades, “L'encarregat del tractament en el Reglament General de Protecció de Dades” (RGPD), (2018), disponible en: [http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament\\_general\\_de\\_proteccio\\_de\\_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf](http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf), visitado el 20-03-2019.



*sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea*".<sup>45</sup> Esta es una clara mejoría respecto de regulaciones anteriores, ya que la presente no se basa "en la condición del uso de medios ubicados en el territorio".<sup>46</sup>

---

<sup>45</sup> MAYOR GÓMEZ, Roberto, "Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)", *Gabilex* Nº 6, (2016), p. 11, disponible en [http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revista\\_gabilex\\_no\\_6\\_autor\\_roberto\\_mayor\\_gomez.pdf](http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revista_gabilex_no_6_autor_roberto_mayor_gomez.pdf), visitado el 18-12-2018.

<sup>46</sup> DURÁN ARROYO, Alicia "El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito." *UAM Revista Jurídica Universidad Autónoma de Madrid*, Nº 37, (2018), p. 425, disponible en: <https://revistas.uam.es/revistajuridica/article/view/10227>, visitado el 18-12-2018.

## **IV. Principales claves del Reglamento**

En este apartado se analizarán aquellos puntos del Reglamento que cabe destacar, ya sea por la entidad y relevancia que poseen o porque suponen una novedad a tener en cuenta respecto a regulaciones anteriores.

### **IV.A. El consentimiento**

Sin duda, la figura del consentimiento es clave en el ámbito del presente Reglamento, donde aparece regulado principalmente en el séptimo de sus artículos. Pero antes de adentrarse en dicho tema, es necesario tener en cuenta la definición que realiza el RGPD en su cuarto artículo, apartado once:

*“Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”.*

En base a este concepto se estructurará el presente apartado, atendiendo a que sintetiza los caracteres más importantes del consentimiento, entre los cuales se extraen los siguientes: la necesaria libertad y por ende ausencia de coacción; la concreción de los datos cuyo tratamiento va a tener lugar; el derecho a la información del interesado sobre la forma en que va a versar ese tratamiento; y por último la aceptación que debe suponer un consentimiento sin lugar a duda, es decir, expreso.

La regulación de la protección de datos ha sufrido un cambio considerable, puesto que en la actualidad para entenderse que existe consentimiento del interesado es necesario probar que éste consintió expresamente en base a una declaración o acción positiva del interesado en el tratamiento de sus datos personales por una entidad concreta y para un fin o fines específicos. Por ende, la realización de un consentimiento tácito ya no basta, considerándose como insuficiente el mero silencio o inacción.<sup>47</sup> Ello se traduce en la práctica tal y como

---

<sup>47</sup> MAYOR, *op. cit.*, p. 13.

Aparicio Vaquero refleja: “*tras haber recibido la oportuna información: adiós a las casillas premarcadas («si no desea que sus datos sean tratados, desmarque esta casilla») como práctica extendida que existe actualmente*”.<sup>48</sup>

De este modo, en aras de probar la existencia de dicho consentimiento, el responsable deberá poder acreditar que tuvo lugar la aprobación del interesado después de habersele ofrecido toda la información correspondiente, de forma fácilmente entendible y libremente. Además, en aquellos casos en que el consentimiento se dé dentro del marco de otras operaciones de diversa índole, este debe ser claramente distinguible. En este sentido, tal y como refería la Vicepresidenta de la Comisión Europea Viviane Reding “*la carga de la prueba debe estar en los controladores de datos, los que procesan sus datos personales*”.

49

Además, cabe tener en cuenta que este consentimiento expreso y consciente no solo abarca los datos que quieran recabarse con posterioridad a la entrada en vigor del Reglamento, sino que también incluye datos personales que las empresas u organismos ya hayan recabado con anterioridad y sigan teniendo en su poder.

Se requiere, en casos determinados, que el consentimiento tenga el carácter de explícito, reforzándose aún más la expresa aceptación del tratamiento de determinados datos personales por entenderse como considerablemente sensibles. Estos definen aspectos de la esfera más privada del individuo como su origen racial o étnico, ideologías políticas, creencias o enfermedades. Por regla general, su tratamiento está prohibido,<sup>50</sup> pero ello puede ser salvado si el interesado en cuestión ofrece su consentimiento de manera explícita. Aun así, este extremo está limitado, ya que el mencionado consentimiento solo podrá tener lugar siempre y cuando el Derecho Comunitario o los Estados Miembros no lo prohíban.

---

<sup>48</sup> APARICIO VAQUERO, Juan Pablo, “La protección de datos que viene: el nuevo Reglamento General europeo”, *Ars Iuris Salmanticensis Tribuna de actualidad* Vol. 4, (2016), p. 29, disponible en: <http://revistas.usal.es/index.php/ais/article/view/15752>, visitado el 23-01-2019.

<sup>49</sup> DÍAZ, Efrén, “El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi Doctrinal*, Nº 6, (2016), p. 15, disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=5652263>, visitado el 17-11-18.

<sup>50</sup> Así se establece en el artículo 9 del RGPD, DO L 119 de 4.5.2016, p. 1/88.

En lo que concierne a la retirada del consentimiento, esta podrá llevarse a cabo en el momento que así se desee y sus datos deberán ser suprimidos sin mediar dilación, de acuerdo con el artículo 17.1. En todo caso, se establece que la acción de retirar el consentimiento debe presentar la misma facilidad que ofrecerlo.

La figura del consentimiento, tomado desde el punto de vista de los menores es también parte importante del RGPD, atendiendo a que los menores son, y así lo establece el considerando número 38, un colectivo que merece especial protección. Dada su vulnerabilidad fundada en la menor consciencia que pueden tener sobre los riesgos del tratamiento de sus datos personales, se les otorga una protección específica, especialmente en la utilización de estos en fines como la mercadotecnia o la creación de perfiles.

Dicha importancia queda demostrada en la dedicación de un artículo íntegro como es el octavo. En dicho precepto, se establece que, para considerarse lícito, el consentimiento sobre el tratamiento de datos de un menor debe haberse otorgado por un niño de al menos 16 años. En caso de que no los haya cumplido, el encargado de realizar el consentimiento será el padre o el tutor legal.

De forma subsidiaria, los Estados Miembros están facultados para reducir la edad a partir de la cual el consentimiento de los menores referente al tratamiento de sus datos personales es válido. Aunque esta facultad presenta una limitación, y es que dicha edad no puede ser inferior a 13 años. De nuevo, el responsable del tratamiento es quien ostenta la carga de la prueba, por ende, deberá asegurarse que el consentimiento se realizó siguiendo estos parámetros y especialmente al dirigirse en un público menor, el lenguaje utilizado deberá ser comprensible al entendimiento de los niños. A modo de ejemplo, en el caso español, es necesario tener al menos catorce años.<sup>51</sup>

---

<sup>51</sup> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857, artículo 12.6

#### **IV.B. Los derechos del interesado**

En el tercer capítulo del Reglamento se establecen los diferentes derechos de los que dispone el interesado en aras de hacer valer la protección de sus datos personales:

En primer lugar, en virtud de la **transparencia** promulgada en el artículo 12, el responsable deberá remitir al interesado toda información relevante para el caso en los términos del RGPD y en especial de sus artículos 13 y 14, a modo de ejemplo se incluyen la identidad y contacto del responsable, o los fines a los que se destina el tratamiento en cuestión.

Otro de los derechos enunciados es el referente al **acceso** del interesado, mediante el cual es posible conocer si unos datos personales se están tratando y una serie de información referente a los fines a los que se destinan, su categoría, sus destinatarios, el plazo para su conservación o la transmisión a terceros.

También cabe mencionar el derecho a la **rectificación**, en virtud del cual el interesado estará facultado para exigir la corrección de sus datos personales objeto de tratamiento para así salvaguardar su exactitud con la realidad.

En relación con el anterior, uno de los derechos más importantes mencionados en el presente capítulo es sin duda el **derecho al olvido**, el cual ha sido positivizado en el Reglamento objeto de estudio a raíz de resoluciones como la STJUE de 13 de mayo de 2014.<sup>52</sup> A la misma se hará referencia de forma más detenida con posterioridad, sin embargo, dada la repercusión que dicha resolución tuvo y lo importante que ha sido para la posterior inclusión del derecho en el RGPD, cabe realizar aquí una pequeña síntesis.

---

<sup>52</sup> Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12, Google Spain, S.L., Google Inc. vs Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317.

El origen de la mencionada resolución tuvo lugar a partir de que la Sala de lo Contencioso-Administrativo de la Audiencia Nacional<sup>53</sup> planteara a la Gran Sala del Tribunal de Justicia de la Unión Europea una cuestión prejudicial, todo ello en el contexto del asunto Google Spain S.L c. Agencia Española de Protección de Datos. En este caso para salvaguardar la indefensión generada por los motores de búsqueda en internet se les atribuían ciertas responsabilidades en el ámbito de la protección de datos personales.

En este sentido, los responsables de dichos buscadores están obligados a respetar el derecho de olvido, basado en los derechos de oposición y cancelación, con lo cual, si una persona fundamenta que existen en la Red datos que vulneran sus derechos puede solicitar que estos desaparezcan.

Fue, por tanto, una sentencia básica para el posterior desarrollo de la protección de datos, y en especial del RGPD. La autora Dopazo Fraguío expresa en los siguientes términos la importancia de dicha resolución: *“esta STJUE fue determinante para estimar que era necesario fijar una regulación eficaz con el fin de tutelar el DPD en la Unión Europea. Y en este sentido, esta STJUE ha sido valiosa para, propiciando una doctrina jurisprudencial que ha sido clave en este ámbito, de utilidad para orientar o impulsar el nuevo RGPDE, que de forma expresa integra esta doctrina; y a su vez para encaminar el diseño de protocolos de actuación”*.<sup>54</sup>

Sin embargo, esta no es la única sentencia que ha supuesto un desarrollo del derecho al olvido en el ámbito europeo: la STJUE de 9 de marzo de 2017,<sup>55</sup> aunque revestida de menor importancia, ofreció una concreción del derecho al olvido en lo que concierne a la información registral. Tal resolución propuso una ponderación de derechos, interesante para observar el razonamiento que debe efectuarse cuando algún derecho fundamental colisiona con el derecho al olvido, que como no podía

---

<sup>53</sup> Auto de la Audiencia Nacional de 27 de febrero de 2012 (RJCA 2012, 321).

<sup>54</sup> DOPAZO FRAGUÍO, María Pilar, “La protección de datos en el Derecho Europeo: Principales aportaciones doctrinales y marco regulatorio vigente. (novedades del Reglamento General de Protección de Datos)”, *Revista Española de Derecho Europeo*, Nº 68, (2018), p. 138.

<sup>55</sup> ECLI:EU:C:2017:197

ser diferente es limitado y en este supuesto vencido por el interés general en el ámbito de la información registral.

En virtud de la primera de las resoluciones mencionadas, el artículo 17 del RGPD reconoce este derecho al olvido, al que también denomina derecho de supresión, definiéndolo como facultad cuyo ejercicio supone la supresión de los datos personales por parte del responsable del tratamiento, el cual debe llevarse a cabo sin dilación indebida, término que por su ambigüedad supone que no exista un tiempo fijado para la eliminación de los mismos.

En todo caso, este derecho únicamente podrá ejercitarse en los supuestos expresamente marcados: cuando ya no tenga sentido conservarlos por el fin para el que fueron recogidos o fueran tratados ilegalmente; cuando el interesado retire su consentimiento, o se oponga al tratamiento; cuando la supresión obedezca a una obligación legal determinada por el Derecho Europeo o de los Estados Miembros, incluidas las referentes al consentimiento del menor.

Pero tal derecho no cuenta únicamente con la limitación que supone su aplicación en casos tasados, sino que, además, incluso cuando concurren los supuestos anteriormente referenciados podrá negarse el derecho al olvido si es contrario a la libertad de expresión o de circulación, a obligaciones legales, al interés público, a la investigación científica o histórica, o al ejercicio, defensa o formulación de una reclamación. Algunos autores entienden que estas limitaciones deberían presentar un sistema de contralimitación capaz de suponer una salvaguarda para la protección de datos en determinados supuestos y siempre que concurrieran circunstancias especiales, por ejemplo en el caso de los menores *“quizá habría que introducir de lege ferenda matices o una contralimitación o excepción de cara a la protección de los datos del menor que fueron recabados cuando éste no tenía la suficiente madurez para opinar o bien decidir, y que en un momento posterior se puede encontrar con el tratamiento de los mismos y que no*

*puede suprimirlos con carácter general respecto a los fines de investigación científica”.*<sup>56</sup>

Otra de las limitaciones del derecho al olvido es que el responsable del tratamiento está obligado a realizar la suspensión de datos de acuerdo con la tecnología disponible y el coste de su implementación, adoptando en todo momento medidas razonables. Ello ha implicado que parte de la doctrina critique al presente Reglamento a raíz de entender que la redacción final no está a la altura de las pretensiones del mismo, teniendo en cuenta que aspiraba a convertir Europa en un territorio excepcionalmente protector del derecho a la vida privada.<sup>57</sup>

Después de analizar el derecho al olvido desde un punto de vista teórico cabe examinarlo a partir de una óptica más próxima a la práctica judicial.<sup>58</sup> En este sentido, el derecho en cuestión puede ejercerse directamente contra el motor de búsqueda de internet en cuestión, sin tener que realizar acción previa contra el editor original. De hecho, existen en la actualidad formularios habilitados para la mayoría de los buscadores más reconocidos. Aun así, dicha información frente a la cual se pretende la supresión no será eliminada de las fuentes del buscador, ni tampoco de la fuente original. Lo que se va a conseguir si la acción prospera es que el enlace en cuestión dejará de aparecer visible cuando se realice una búsqueda en internet usando el nombre de la persona cuyo derecho quiere hacerse valer, pero si esta acción se ejercita contra el buscador el resultado seguirá apareciendo en Internet cuando la búsqueda se realiza utilizando otros términos diferentes del nombre del perjudicado.

---

<sup>56</sup> SARRIÓN J. Esteve, “Las novedades de la nueva normativa de protección de datos y su aplicación a los ensayos clínicos con menores”, *Derecho y salud, (Ejemplar dedicado a: XXVI Congreso 2017: Derechos sanitario y ciudadanía europea: los retos)*, Vol. 27, Nº Extra 1, (2017), p. 235, disponible en <https://dialnet.unirioja.es/descarga/articulo/6334698.pdf>, visitado el 28-01-2019.

<sup>57</sup> MORITZ Marcel y GIBELLO Valentín, “El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro”, *Revista de Derecho*, Nº 27, (2017), p.121, disponible en <http://repositorio.uasb.edu.ec/handle/10644/5948> visitado el 20-11-18.

<sup>58</sup> Para ello ha sido especialmente tomada en consideración la sede electrónica de la Agencia Española de Protección de Datos, especialmente su página dedicada al Derecho de supresión ("al olvido"): buscadores de internet, disponible en <https://www.aepd.es/areas/internet/derecho-al-olvido.html> visitada el 28-01-2019.



Otros de los derechos que es incorporado al RGPD de forma novedosa es el que concierne a la **limitación** del tratamiento. Tal derecho se caracteriza por llevar a cabo no la eliminación de los datos, sino que se restringe su tratamiento mientras se siguen conservando. Ello implica que tal derecho pueda ser ejercitado únicamente en cuatro supuestos tasados: en primer lugar, cuando el interesado impugne la exactitud de dichos datos, hasta que los mismos sean verificados por el responsable; también cuando el interesado haya manifestado su oposición al tratamiento, pero aun así el responsable del tratamiento considere que concurren motivos legítimos para continuar con el tratamiento; en tercer lugar, podrá ejercitarse dicho derecho en aquellos supuestos en que el interesado precise sus datos personales para cualquier acción relacionada con una reclamación, aunque sean innecesarios para el tratamiento; finalmente la posibilidad del ejercicio del derecho mencionado también concurre cuando aun siendo un tratamiento ilícito, el interesado opta porque sus datos se conserven.

Otro de los nuevos derechos que se incorporan a la normativa europea a raíz del nuevo Reglamento es el referente a la **portabilidad** de los datos, en este caso, a diferencia de los derechos anteriormente señalados, más centrados en el amparo de la libertad informática, en el derecho a la portabilidad lo que está en juego es la libre competencia.<sup>59</sup> Atendiendo a la gran cantidad de información de la que abastecemos a las empresas en la actualidad, este derecho permite la recepción de los datos personales del interesado en un formato de uso común para posibilitar la transferencia de los mismos a un tercero, todo ello sin que el responsable anterior pueda negarse. Incluso se prevé que cuando la tecnología lo permita, estos datos personales puedan ser transmitidos directamente de un responsable a otro, sin tener que mediar el interesado.

Pese a que los derechos que se han destacado reconocen facultades ciertamente interesantes y algunas de ellas innovadoras, cabe tener en cuenta que son en todo momento derechos limitados, tal y como establece el artículo 23 del RGPD. Sin embargo, las aludidas limitaciones son comprensibles y predecibles

---

<sup>59</sup> FERNÁNDEZ VILLAZÓN, Luis Antonio, “El nuevo Reglamento Europeo de Protección de Datos”, *Foro Nueva época*, vol. 19, N° 1, (2016), p. 401, disponible en <http://dx.doi.org/10.5209/FORO.53399>, visitado el 29-01-2019.

como la seguridad del Estado o pública, la defensa, lo relativo a ciertos procesos judiciales desde su fase preventiva hasta la ejecutiva, o el interés público.

#### **IV. C. El Delegado de Protección de datos**

Otra de las novedades introducidas por el Reglamento en cuestión es la del Delegado de Protección de datos, aunque debe tenerse en cuenta que la anterior Directiva ya preveía la posibilidad de nombrar a un “controlador”, que únicamente fue reconocido en Alemania, en base a la Ley Federal Alemana de Protección de Datos.<sup>60</sup>

La figura del Delegado de Protección de Datos es equiparable a la de un “auditor interno”<sup>61</sup> dedicado a la materia de la protección de datos. Las funciones del mismo residen en llevar a cabo el asesoramiento de la protección de datos, indicando al responsable, el encargado del tratamiento o cualquier empleado que se ocupe de este, las directrices que debe seguir en aras de cumplir con la vigente normativa; lo cual incluye también asegurarse que la entidad en la que lleva a cabo sus servicios respeta el Reglamento, todo ello cumpliendo con su deber de colaborar con la autoridad de control, frente a la cual puede dirigir consultas.

En este sentido, el responsable y el encargado del tratamiento deben escoger a un Delegado caracterizado por poseer unos conocimientos tanto técnicos como jurídicos en relación con la protección de datos y desempeñe con confidencialidad sus funciones. Asimismo, dicho Delegado deberá reunir el requisito indispensable de imparcialidad, de modo que no puede verse supeditado a las órdenes del responsable ni del encargado, los cuales no tienen potestad para sancionarle o destituirle en el marco del ejercicio de su labor. Por ende, su relación podrá darse en el ámbito de un contrato de servicios o directamente revistiendo el carácter de empleado.

---

<sup>60</sup> SARRIÓN, *op. cit.*, p. 235.

<sup>61</sup> FERNÁNDEZ, *op. cit.*, p. 405.

Todo ello implica que el Delegado de Protección de Datos cumple unas funciones de aseguramiento del cumplimiento del RGPD, así como de cualquier otra normativa referente a esta materia. Incluso está capacitado para asignar responsabilidades, concienciar y formar al personal participante en el tratamiento y las auditorías correspondientes.<sup>62</sup>

Sin embargo, pese a llevar a cabo una importante labor, contar con un Delegado de Protección de Datos no es siempre preceptivo. El artículo 37 establece las situaciones en las cuales deberá designarse a uno: primeramente, cuando el tratamiento corra a cargo de una autoridad u organismo público; en segundo término, cuando las principales actividades del responsable o encargado sean a gran escala y por tanto necesiten una vigilancia constante; y en tercer lugar cuando dichas actividades estén relacionadas con categorías especiales de datos personales.

En aras de facilitar la implantación del Delegado de Protección de Datos en el mayor número de entidades posible, se prevé la posibilidad de que un grupo empresarial pueda nombrar un único Delegado que deberá desarrollar sus funciones en cada establecimiento. De modo similar, las autoridades u organismos públicos podrán hacer lo propio, compartiendo Delegado siempre y cuando ello sea posible en virtud de su estructura y tamaño.

En el ámbito español, la Agencia Española de Protección de Datos ha decidido promover un sistema de certificación profesional que podrá utilizarse a fin de evaluar objetiva e imparcialmente a aquellas personas físicas o jurídicas que se presenten con intención de ocupar el puesto de Delegado de Protección de Datos.<sup>63</sup>

Por lo tanto, a modo de resumen, el Delegado de Protección de Datos “*viene a reforzar los derechos de los interesados, implicando a su vez un mayor nivel de responsabilidad y cuidado por parte de las empresas*” puesto que reside en su

---

<sup>62</sup> Tal y como establece la Agencia Española de Protección de Datos en su sede electrónica <https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00061>

<sup>63</sup> Agencia Española de Protección de Datos, esquema de certificación de delegados de protección de datos, (2018), disponible en <https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf>, visitado el 12-11-2018.

figura el deber de “*rendir cuentas “directamente al más alto nivel jerárquico” de la organización empresarial*”.<sup>64</sup>

#### **IV.D. Las autoridades de control**

El RGPD obliga a todo Estado Miembro a determinar autoridades públicas independientes, pueden ser varias o una sola, cuya función sea principalmente asegurarse del cumplimiento del Reglamento en el ámbito de su territorio, colaborando en todo momento entre ellas y junto a la Comisión. Tales autoridades reciben el nombre de autoridades de control.

Cabe decir que se otorga cierta autonomía a los Estados en lo que concierne a las autoridades de control, estableciendo una libertad limitada en lo referente al nombramiento de los miembros de estas, los requisitos de estos deben cumplir, sus obligaciones y la duración de su mandato, el establecimiento de la autoridad o las competencias que asume.

Como se ha dicho, pueden existir diversas autoridades en un mismo Estado Miembro, en cuyo caso se deberá establecer una encargada de representar a las demás en el Comité. En cualquier caso, cada autoridad desempeñará sus funciones en el territorio en el que se sitúe, pudiendo entrar a conocer únicamente aquellos casos relacionados con el tratamiento de datos llevado a cabo por organismos públicos o privados establecidos en su país.

Sin embargo, las autoridades de control ostentan más funciones además de supervisar que el RGPD sea aplicado. En efecto, también les incumben las tareas de información a la ciudadanía de los peligros que incumben al tratamiento de datos personales, con especial enfoque hacia los menores como sujetos especialmente desprotegidos; en este sentido, se permite a los interesados realizar consultas frente a las autoridades, que deberán proveerles de la información relacionada; dichas

---

<sup>64</sup> PADÍN, Alejandro, “Reglamento General de Protección de Datos de la UE: una visión desde el periodo de adaptación”, *Actualidad Jurídica Aranzadi* N° 925, (2016), p.2, disponible en [https://www.garrigues.com/es\\_ES/noticia/reglamento-general-de-proteccion-de-datos-de-la-ue-una-vision-desde-el-periodo-de-adaptacion](https://www.garrigues.com/es_ES/noticia/reglamento-general-de-proteccion-de-datos-de-la-ue-una-vision-desde-el-periodo-de-adaptacion), visitado el 29-01-2019.

labores de sensibilización también versarán sobre los responsables o encargados del tratamiento. Otra de las funciones importantes de que realizan es el asesoramiento frente al Gobierno o Parlamento, en el ámbito de las medidas legislativas y administrativas; también se encargan de investigar tanto las reclamaciones que se le presenten como la aplicación del Reglamento. Respecto a tales reclamaciones, las mismas pueden presentarse por cualquier interesado, sin perjuicio de ejercer otras acciones, siempre y cuando este considere que se han vulnerado su derecho a la protección de datos, a modo de ejemplo, la página web oficial de la Agencia Española de Protección de Datos incluye formularios para facilitar la reclamación a los ciudadanos.<sup>65</sup>

En definitiva, estas son algunas de las funciones de índole más significativa realizadas por las autoridades de control, pero estas son muy amplias debido al sistema de *numerus apertus* previsto en el artículo 57.1 letra v). Aun así, de todas ellas pueden beneficiarse el Delegado de Protección de Datos y los interesados sin coste económico alguno por regla general. Se prevé como posible llevar a cabo acciones contra la propia autoridad de control frente a las resoluciones jurídicas vinculantes que esta haya dictado.

Llegados a este punto, cabe destacar la importante labor realizada por la Agencia de Protección de Datos Española,<sup>66</sup> la cual ha supuesto una gran aportación en favor de la protección de datos y más específicamente del derecho al olvido.

#### **IV. E. El ámbito de la responsabilidad**

En los supuestos donde se entienda que ha existido vulneración de los datos personales amparadas por el Reglamento objeto del presente análisis, existen dos soluciones de índole distinta. La primera ha sido tratada en el punto anterior, referente a las reclamaciones que pueden presentarse a las autoridades de control,

---

<sup>65</sup> Agencia Española de Protección de Datos, presentación de reclamación, disponible en <https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/solicitudReclamacion.jsf;jsessionid=mnWhSvyzqN1rxVTSAVD7zop9> visitado el 10-04-2019.

<sup>66</sup> Tal y como resalta DOPAZO, “La protección de datos en el Derecho Europeo: Principales aportaciones doctrinales y marco regulatorio vigente. (novedades del Reglamento General de Protección de Datos)”, p. 124.

tratándose así de una vía administrativa para la resolución del conflicto que puede derivar en el ámbito judicial.

Por otra parte, encontramos las acciones judiciales que se realizan por cualquier persona de modo directo frente a los responsables del tratamiento de datos o los encargados, por incumplimiento de sus obligaciones derivada en una infracción del Reglamento que vulnere el legítimo tratamiento de datos de una persona, causando perjuicios, ya sean materiales o inmateriales. Sin embargo, el encargado únicamente responderá no solo cuando incumpla sus obligaciones sino también en aquellos casos donde haya desobedecido las órdenes del responsable. Aún así, ambos sujetos estarán exentos de responsabilidad en caso de que demuestren que no han sido los causantes de los perjuicios.

Este proceso se realiza con el fin de establecer una resolución favorable para el interesado que implique, entre otras, la limitación o prohibición del tratamiento. Tales acciones no podrán presentarse nunca frente a una autoridad de control, en los términos ya mencionados.

En este sentido, el RGPD realiza una importante mejora respecto a la anterior regulación comunitaria, también en relación con los órganos competentes de resolver: *“los perjudicados pueden optar entre acudir a los tribunales de cualquier EM en el que el responsable o encargado tengan un establecimiento, o bien a los tribunales en los que el interesado tenga su residencia habitual, esto último salvo que el responsable o encargado sea una autoridad pública de un EM que actúe en el ejercicio de sus poderes públicos”*.<sup>67</sup>

Frente a las infracciones, se prevé un sistema de multas administrativas que el Reglamento articula para aquellos supuestos en que se infrinja la protección de datos personales. En este ámbito las autoridades de control deberán cumplir con la importante labor de garantizar que las mencionadas multas cumplan con tres requisitos esenciales: efectividad, proporcionalidad y disuasoriedad. Su imposición

---

<sup>67</sup> DURÁN, *op. cit.*, p. 430.

podrá añadirse a las medidas de investigación previstas a favor de dichas autoridades de control o establecerse como sustitución de las mismas.

En todo caso, se estima preceptivo para el cálculo de la cuantía final la estimación de una serie de factores como la duración de la infracción, la intencionalidad, la gravedad, la cantidad de afectados, las medidas tomadas para reducir los daños, la cooperación con autoridades de control, el grado de responsabilidad en relación con las medidas técnicas u organizativas que debieron tomarse, la existencia o no de infracciones anteriores por parte de los mismos sujetos, la clase de datos personales que se vieron afectados, si la infracción fue notificada, si se impusieron medidas previas al infractor, la adhesión a códigos de conducta,<sup>68</sup> o los beneficios que ha supuesto dicha infracción.

Las sanciones que esta norma prevé la dotan de una mayor efectividad respecto a anteriores regulaciones,<sup>69</sup> a modo de ejemplo, las sanciones previstas para infracciones graves pueden alcanzar los diez millones de euros o el dos por ciento de la facturación mundial en el ejercicio anterior. Por otra parte, las infracciones muy graves supondrán multas de hasta veinte millones de euros o el cuatro por ciento de la facturación mundial.

Para concluir el presente apartado referente a la regulación de la responsabilidad y las sanciones en el ámbito del Reglamento, considero interesante la reflexión que se realiza por parte de la doctrina,<sup>70</sup> enfatizándose la relevancia de esta norma, no únicamente en lo que respecta a la cuantía de las sanciones establecidas sino también destacando lo que supone para las entidades, ya que a éstas se les atribuye la obligación de señalar los puntos de riesgo y tomar las medidas necesarias para paliarlo.

---

<sup>68</sup> En virtud del artículo 40 del RGPD son códigos cuya función reside en contribuir a la correcta aplicación del Reglamento atendiendo a las peculiaridades de cada sector del tratamiento.

<sup>69</sup> MINERO, “Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea”, p. 24.

<sup>70</sup> BIURRUN ABAD, Fernando J., “Accountability o responsabilidad activa en el Reglamento General de Protección de Datos”, *Actualidad Jurídica Aranzadi* N° 927, (2017), p. 1.

## **V. Análisis de la jurisprudencia de interés**

La Jurisprudencia europea ha contribuido especialmente en el desarrollo de una buena parte de los elementos plasmados en el RGPD, así lo admite la doctrina,<sup>71</sup> que mayoritariamente destaca algunas resoluciones por encima de las demás. En concreto, las sentencias más destacadas en el ámbito reciente de la protección de datos europea son la Sentencia del Tribunal de Justicia de 13 de mayo de 2014 referente al asunto Google Spain S.L c. Agencia Española de Protección de Datos y la Sentencia del Tribunal de Justicia (Sala Segunda) de 9 de marzo de 2017<sup>72</sup>.

### **V.A. Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014**

Los hechos que dieron origen a esta importante resolución se remontan al 5 de marzo del año 2010, año en que Don Costeja González decidió interponer una reclamación ante la Agencia Española de Protección de Datos, por considerar que el portal electrónico de uno de los periódicos más reconocidos a nivel nacional había vulnerado sus derechos al publicar una noticia en la que se embargaban algunos de sus bienes como resultado del impago a la seguridad Social.

Sin embargo, dicha reclamación se dirigió no solamente contra el periódico sino también frente a Google Spain y Google Inc., por ser el motor de búsqueda en el que con una sencilla búsqueda de su nombre aparecía la noticia en cuestión. Con el objetivo de que tal situación cesara, Costeja pidió a las entidades mencionadas que suprimieran estos datos personales de internet, puesto que la noticia se remontaba a 1998 y ya había puesto fin a sus problemas económicos.

La AEPD resolvió desestimando la reclamación frente al periódico, pero la estimó en lo que respectaba a Google Spain y Google Inc, al considerarlos sometidos a la normativa de protección de datos. Hecho que motivó a las empresas

---

<sup>71</sup> DOPAZO, *op. cit.*, p.138.

<sup>72</sup> Sentencia del Tribunal de Justicia de la Unión Europea de 9 de marzo de 2017, asunto C 398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni ECLI:EU:C:2017:197



tras los motores de búsqueda a presentar un recurso ante la Audiencia Nacional, en adelante denominada AN. El mencionado órgano judicial presentó una cuestión prejudicial frente al TJUE cuya resolución sería otorgada con la sentencia objeto de estudio en el presente apartado del trabajo.

En esencia, la duda de la AN venía motivada por las obligaciones que la normativa del momento, en este caso la Directiva 95/46, exigía a los motores de búsqueda respecto a los datos cuya supresión se solicitaba por un perjudicado, ¿cuál debía ser la postura de tales motores frente demanda de eliminar datos personales de la web de un tercero? A ello responde el TJUE en los siguientes términos:

En primer lugar, debe interpretarse que del supuesto enjuiciado se desprende un claro tratamiento de datos personales llevado a cabo por un establecimiento del responsable, siendo preceptiva la aplicación de la normativa europea al disponer Google de una filial situada en un Estado Miembro cuya actividad repercute en los ciudadanos de este.

Asimismo, la actividad de los motores de búsqueda se considera tratamiento por la mencionada resolución: *“la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de tratamiento de datos personales”*;

En segundo término, el motor de búsqueda demandante tiene el deber de eliminar de la lista de resultados aquellos datos personales que el Sr. Costeja solicita suprimir, puesto que tal y como establece la Sentencia: *“incumbe al responsable del tratamiento garantizar que los datos personales sean «tratados de manera leal y lícita», que sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines», que sean «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente», que sean «exactos y, cuando sea necesario, actualizados», y, por último, que sean «conservados en una forma que permita la identificación de los interesados durante un período no superior al*

*necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente”.*

Asimismo, se determina la prevalencia del derecho del interesado a que cierta información perjudicial para su persona desaparezca del resultado de una búsqueda en internet, por encima no solo de los intereses económicos que correspondan al gestor del motor de búsqueda, sino también del derecho a la información.

De este modo, la doctrina mayoritaria entiende que se consagra el derecho al olvido, aunque existen opiniones minoritarias que lo entiendan de modo distinto al considerar que el TJUE no crea el derecho al olvido, sino que únicamente ofrece la posibilidad de que solicitar la eliminación de ciertos resultados ofrecidos por los buscadores<sup>73</sup>. Aun así, la rama doctrinal mayoritaria respalda que el derecho a la protección de datos a partir de la resolución citada pasaría de ser un hipotético derecho fundamental a una realidad,<sup>74</sup> que posteriormente sería consagrada en el Reglamento objeto del presente trabajo.

## **V. B. Sentencia del Tribunal de Justicia (Sala Segunda) de 9 de marzo de 2017**

Siguiendo con la jurisprudencia anteriormente referenciada sobre el derecho al olvido, la presente sentencia indaga aún más en el mismo, estableciendo, en los términos que serán expuestos, ciertas limitaciones. En cierta manera podría decirse que mientras el asunto C-131/12 consagra el derecho al olvido, especialmente en el ámbito digital, el caso C-398/15 determina sus límites. El supuesto de hecho en el que nace la controversia es el siguiente:

---

<sup>73</sup> KULK Stefan y ZUIDERVEEN Borgesius, “Google Spain v. González: Did the Court Forget about Freedom of Expression?”, *European Journal of Risk Regulation*, (2014), p.12, disponible en <https://ssrn.com/abstract=2491486>, visitado el 14-02-19.

<sup>74</sup> MARTÍNEZ LÓPEZ-SÁEZ, Mónica, “Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: la difícil conciliación entre las libertades económicas y la protección de datos personales”, *Revista Estudios Deusto*, vol. 65/2, (2017), p. 176, disponible en [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKewiM\\_ut3pDgAhWfAGMBHeDsDDcQFjAlegQIAhAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6304834.pdf&usg=AOvVaw3AmWhhr4tN3gFxuWuB-7Wu](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKewiM_ut3pDgAhWfAGMBHeDsDDcQFjAlegQIAhAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6304834.pdf&usg=AOvVaw3AmWhhr4tN3gFxuWuB-7Wu), visitado el 14-02-19.

Don Salvatore Manni, solicitó a la Cámara de Comercio de Lecce que suprimiera una serie de datos personales del registro de sociedades que le estaban perjudicando en la actualidad. En concreto, Manni había sido en el pasado administrador único y liquidador de una sociedad declarada en concurso de acreedores, pero ello tuvo lugar en 1992, con lo cual la defensa de Manni entendió que había transcurrido tiempo más que suficiente para proceder a la eliminación de esos datos personales que en la actualidad seguían perjudicando a los proyectos comerciales de su principal.

Frente a tales hechos, el Tribunal di Lecce italiano estimó sus pretensiones, condenando a la Cámara de Comercio de Lecce a hacer anónimos los datos que relacionaban al actor con la liquidación de su anterior sociedad e indemnizarle por los daños y perjuicios sufridos.

Sin embargo, el asunto fue objeto de recurso frente al Tribunal Supremo de casación italiano, órgano encargado de elevar la cuestión prejudicial y así permitir al TJUE seguir desarrollando jurisprudencialmente el derecho al olvido. En síntesis, la duda del Tribunal italiano residía en si los Estados Miembros están facultados o incluso obligados para otorgar a las personas físicas la capacidad de solicitar a las autoridades competentes para el registro de sociedades la limitación del acceso a determinados datos personales tras el transcurso de un tiempo.

Tras el debido análisis de las dos normas en conflicto, es decir, la Directiva 68/151/CEE en su versión modificada por la Directiva 2003/58/CE<sup>75</sup> por una parte, y la ya referenciada anteriormente Directiva 95/46/CE por otra; el TJUE entiende que los datos que figuran en los registros societarios son, sin duda, personales, no pierden su condición por estar asociados a la actividad de una persona jurídica. Asimismo, las entidades encargadas de controlar el registro llevan a cabo un tratamiento de los mismos, con lo cual se consideran responsables. Finalmente, el TJUE atribuye a los Estados Miembros la importante labor de establecer caso por

---

<sup>75</sup> Directiva 68/151/CEE del Consejo, de 9 de marzo de 1968, Primera Directiva tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades definidas en el segundo párrafo del artículo 58 del Tratado, para proteger los intereses de socios y terceros (DO 1968, L 65, p. 8; EE 17/01, p. 3), en su versión modificada por la Directiva 2003/58/CE del Parlamento Europeo y del Consejo, de 15 de julio de 2003 (DO 2003, L 221, p. 13)

caso frente a qué supuestos cabe la petición de las personas físicas ante a la autoridad responsable del registro. Sin embargo, los insta a únicamente conceder tal permiso bajo una serie de condiciones y estrictamente en casos que cumplan ciertos requisitos, concretamente cuando esté “*especialmente justificado por razones preponderantes y legítimas*”, siendo además preceptivo que haya transcurrido un tiempo suficientemente largo desde la disolución de la sociedad anterior.

Ello implica que, en caso de cumplirse lo establecido, el acceso a dichos datos personales que hayan sido inscritos en el registro sea limitado exclusivamente a quienes acrediten un interés específico en su consulta. Por lo tanto, esta resolución elabora una concreción del derecho al olvido, estableciendo ciertas limitaciones respecto a otros derechos como en este caso es la información registral.

## VI. Conclusiones

Llegados a este punto del trabajo, después de haber analizado el RGPD desde sus antecedentes y habiendo estudiado las resoluciones judiciales que ayudaron a perfilarlo, juntamente con los comentarios y aportaciones doctrinales al respecto, cabe resolver la pregunta inicial que inspiró este análisis, ¿está el Reglamento a la altura de los peligros que acechan actualmente a la protección de los datos personales?

Para ello creo que es necesario abordar el Reglamento desde tres enfoques distintos, la norma en sentido estricto, su aplicación en supuestos reales y el reto que supone internet para la protección de los datos.

De este modo, estructuraré mis conclusiones en los siguientes puntos: primeramente, reflejaré aquellos aspectos destacables del RGPD tanto favorables como mejorables a fin de valorar si se trata de una regulación adecuada; en segundo término analizaré si el Reglamento ofrece en la práctica una protección real de nuestros datos; en tercer lugar trataré de determinar si el RGPD logra proteger los datos de las personas en el actual modelo de internet.

En primer lugar, estimo oportuno partir de la base de que la mencionada norma europea recoge una serie preceptos bien contruidos con pretensiones que sin lugar a duda persiguen la mejora en el ámbito de la protección de datos europea. Además, en comparación con las anteriores normativas que lo precedieron, el actual reglamento presenta un mayor amparo frente a injerencias al ámbito privado de la persona, reflejando normativamente las necesidades que la jurisprudencia iba adelantando en las sentencias analizadas. En otras palabras, desde un punto de vista teórico propone un régimen jurídico “*sólido y uniforme*”.<sup>76</sup>

En este sentido, considero que la aprobación del RGPD era necesaria, puesto que ofrece una serie de garantías que la Directiva 95/46/CE era incapaz de brindar. Esta última era actualmente insuficiente en especial por no garantizar una

---

<sup>76</sup> DOPAZO, *op. cit.*, p. 145.

aplicación uniforme de la protección de datos en Europa. Tal carencia fue suplida por el Reglamento en base a una aplicación de alcance general revestida de obligatoriedad y aplicabilidad en todo Estado Miembro.

Asimismo, el RGPD establece una protección amplia de los datos personales, ya que se ampara toda información de una persona física independientemente de la tecnología empleada en su tratamiento. Ello además implica que por mayor que sea la modernidad de los sistemas utilizados para el tratamiento ninguno de ellos se excluirá de la aplicación del RGPD. De este modo en base a la actual regulación quedan protegidos datos personales que escapaban de la anterior regulación como la ubicación de los dispositivos móviles.

También en el ámbito de los derechos personales considero que se establece un mayor amparo que contribuye en gran manera a configurar una mayor protección de los datos de carácter personal. En efecto, el consentimiento debe ser ahora expreso e inequívoco, siendo insuficiente aquel que se entienda como tácito, además este podrá ser retirado en cualquier momento con toda facilidad. Se prevé también la capacidad de acceder, rectificar y suprimir tales datos personales de un modo que no se había plasmado normativamente hasta la llegada del RGPD.

Entre tales derechos destacaría el referente al olvido, el cual tal y como se establece en el artículo 17 del Reglamento y en base a la jurisprudencia que el Tribunal de Justicia de la UE estableció en el caso Google Spain, deberá tenerse en cuenta por aquellos responsables que hayan hecho públicos datos personales, permitiendo a la persona afectada la supresión de su información privada.

Otro de los puntos para mí más fuertes del RGPD es que amplía el ámbito territorial de protección, aspecto especialmente importante dado que con la anterior regulación si la entidad responsable del tratamiento se establecía fuera del territorio de la Unión era difícil amparar los derechos del ciudadano afectado. A partir del Reglamento, esto cambia, de manera que no solo se garantiza la protección de datos frente al tratamiento realizado por establecimientos situados en la Unión, sino que también cuando estos estén situados fuera de ella se establece una protección que ampara a los residentes en la UE del tratamiento indeseado de sus datos personales.

Aunque ello admita matices, ya que será necesario que tal tratamiento esté relacionado con la Unión, esta ampliación abarca un número mayor de casos anteriormente no amparados por la legislación europea.

En lo que concierne a las sanciones, esta es una novedad que considero refleja la mayor importancia que se quiere otorgar a la protección de datos en Europa. En efecto, el establecimiento de un procedimiento sancionador que ofrece multas de importe elevado, implica para las entidades responsables una mayor preocupación acerca del cumplimiento de la normativa. Ello debería derivar en la aplicación de las medidas necesarias para evitar el incumplimiento del Reglamento.

Como vemos el Reglamento ofrece progresos relevantes, sin embargo, ello no implica que sea perfecto en su totalidad. Del análisis realizado se desprenden varios puntos en los que podría ser mejorable.

En este sentido, el Reglamento no nace únicamente con el objetivo de defender el derecho fundamental a la protección de datos, sino que tiene también un especial interés en la regulación de la libre circulación de datos a fin de simplificarla y agilizar las actividades económicas en la UE. Ello se reconoce expresamente en el propio RGPD al hacer prevalecer la libre circulación de los datos personales por encima de su protección.

Por consiguiente, se implementa el derecho a la portabilidad de los datos personales, ideado no en aras de beneficiar a aquellas personas cuyos derechos se vulneren sino con el objetivo de favorecer la transmisión entre responsables, dado que facilita recepción y transferencia de los datos al exigir el uso de un formato común.

Igualmente, entiendo que el RGPD debería plasmar con mayor concreción los supuestos en que es preceptiva la figura del Delegado de Protección de Datos, puesto que es una cuestión que algunos Estados, entre ellos el español, han tenido que subsanar en sus legislaciones relativas a la protección de datos. De manera análoga el Reglamento ofrece bastante autonomía estatal en lo que concierne a las autoridades de control, especialmente en lo relacionado con su nombramiento y sus

obligaciones. Todo ello impide la consecución de una uniformidad real, lo cual me parece grave dado que tanto los Delegados como las Autoridades de Control son necesarios para asegurar el cumplimiento efectivo del RGPD.

Las imprecisiones e inconcreciones del Reglamento no concluyen aquí, ya que genera cierta inseguridad jurídica con el uso de expresiones como “*no más tiempo del necesario*”. En concreto, el artículo 5.1 e) dispone lo siguiente: “*Los datos personales serán: mantenidos de forma que se permita la identificación de los interesados durante **no más tiempo del necesario para los fines del tratamiento de los datos personales***”. En efecto, la indefinición del concepto puede fácilmente suponer una vulneración para los derechos de la persona cuyos datos son tratados, puesto que no se establece un periodo temporal límite a partir del cual no puede mantenerse tal información.

Lo mismo ocurre con el consentimiento de los menores de edad cuando se indica que los responsables del tratamiento deberán realizar “*esfuerzos razonables*” para cerciorarse que tal consentimiento fue realizado por el titular de la patria potestad o tutela. Al no se ofrecerse mayor concreción sobre qué actuaciones deben llevar a cabo los responsables se facilita que estos puedan llevar a cabo en ciertos casos un aseguramiento insuficiente.

Para sintetizar, creo que las aportaciones del Reglamento son en su mayoría beneficiosas y que en conjunto, aunque cuenta con ciertos elementos que podrían ofrecer una mayor seguridad jurídica, mejora con creces la regulación anteriormente aplicable a la materia.

En segundo lugar, cabe analizar si a partir de la entrada en vigor del RGPD se ha establecido en la práctica una mayor protección de los datos personales, puesto que la verdadera finalidad de cualquier norma debe ser su plasmación efectiva. En este sentido es necesario hacer referencia a algunos casos reales a fin de averiguar qué ha cambiado desde la entrada en vigor del Reglamento.

En el ámbito público, un centro hospitalario situado en Portugal ha sido sancionado por la Agencia de Protección de Datos de dicho país al vulnerar el



principio de integridad y confidencialidad de los datos personales conservados, dado que no contaba con los mecanismos necesarios para la protección de esta información frente a el acceso ilimitado de los trabajadores del hospital al historial clínico de los pacientes.<sup>77</sup>

Este supuesto me ha parecido interesante ya que constata que a partir del RGPD las entidades públicas deberán tener más cuidado en lo referente a la protección de datos, atendiendo a que pueden recibir sanciones tan elevadas como las entidades privadas. Ello a mi parecer es un hecho a tener en cuenta dado que, aunque el Reglamento me parece bastante enfocado en la protección de datos frente a las entidades privadas, este es perfectamente aplicable en el ámbito público, lo cual es importante porque esta clase de entes también disponen de grandes cantidades de información privada que deben ser tratadas conforme al Reglamento.

No obstante, la mayoría de infracciones conciernen a las entidades privadas con un amplio interés comercial en los datos personales. En este sentido, noticias como la adjuntada<sup>78</sup> demuestran que sociedades como Google, siguen siendo señaladas por sus actuaciones contrarias a la protección de datos. En este caso la autoridad francesa de protección de datos multó a dicha compañía por entender que, en esencia, el consentimiento que los usuarios otorgaban para el tratamiento de sus datos personales no era válido.

De este modo, aunque la Unión Europea ha realizado un difícil y meritorio proceso de regulación en este ámbito, no se percibe en la realidad una mayor sensación de seguridad posterior a la aplicación del Reglamento. Ello es porque en cierto modo la vulneración o no de nuestros derechos fundamentales sigue dependiendo de la “buena fe”, especialmente en el caso de las entidades privadas, las cuales no parecen rectificar sus políticas y siguen incumpliendo la normativa aplicable.

---

<sup>77</sup> BAIRRAO, Isabel, “Primeras sanciones en aplicación del RGPD en Portugal” Garrigues digital, disponible en [https://www.garrigues.com/es\\_ES/garrigues-digital/primeras-sanciones-en-aplicacion-del-rgpd-en-portugal](https://www.garrigues.com/es_ES/garrigues-digital/primeras-sanciones-en-aplicacion-del-rgpd-en-portugal), visitado el 01-04-2019.

<sup>78</sup>La Vanguardia, “Francia multa con 50 millones a Google” disponible en <https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html>, visitado el 10-04-2019.

En definitiva, se trata de una buena norma de objetivos, pero que no termina de resolver la fácil vulneración de la privacidad que puede llevarse a cabo actualmente, sobretodo en el ámbito de internet. Un ejemplo de ello uno son las grandes filtraciones de datos que se producen a nivel internacional.<sup>79</sup>

Esta última noticia me sirve para introducir el tercero de los bloques en los que estructuro mis conclusiones, referente a analizar si internet mengua o no la verdadera consecución de las pretensiones del RGPD.

No existe un modelo único de internet, sino que varía considerablemente dependiendo del país, no siendo igual en Rusia que en China, por nombrar dos países especialmente diferenciados. Por ende, es muy complicado proteger nuestros datos personales cuando llegan a según que partes del mundo. En este sentido toma también especial importancia Estados Unidos, país en el que se concentra la soberanía digital, ya que gran parte de los negocios y comercios que se realizan con los datos personales tienen lugar en dicho territorio, tal y como ha podido apreciarse el caso de Google Inc a partir de la STJUE (Gran Sala), de 13 de mayo de 2014.

En aras de buscar una solución a esta importante problemática, considero que el camino a seguir vendría dado a partir de normas como el RGPD que a su vez estuvieran respaldadas por medios tecnológicos capaces de limitar actuaciones fraudulentas, es decir, en mi opinión la protección de datos no puede partir únicamente de normas bien elaboradas, sino que debe acompañarse de escudos tecnológicos capaces de frenar los riesgos actuales. Posiblemente, sería adecuada la creación de varios entes que contaran con tecnología avanzada como “blockchain”, capaz de hacer llegar un aviso a toda persona en caso de que sus datos personales estuvieran siendo usados de forma indeseada. Este sistema, al basarse en operaciones matemáticas, permitiría de forma rápida que toda persona conociera

---

<sup>79</sup> Diario ABC, “Escándalo en Nokia: sus teléfonos han enviado información personal de los usuarios a China”, disponible en [https://www.abc.es/tecnologia/moviles/telefonos/abci-escandalo-nokia-telefonos-enviado-informacion-personal-usuarios-china-201903220229\\_noticia.html#vca=mod-lo-mas-p1&vmc=leido&vso=tecnologia&vli=noticia.foto.tecnologia&vtm\\_loMas=si](https://www.abc.es/tecnologia/moviles/telefonos/abci-escandalo-nokia-telefonos-enviado-informacion-personal-usuarios-china-201903220229_noticia.html#vca=mod-lo-mas-p1&vmc=leido&vso=tecnologia&vli=noticia.foto.tecnologia&vtm_loMas=si), visitado el 29-03-2019

cuándo, en qué lugar, quién ha utilizado sus datos y para qué propósito, permitiendo una reacción automática.

La Unión Europea mostró interés en el “blockchain” al poner en marcha en febrero de 2018 el observatorio y foro de la cadena de bloques de la UE,<sup>80</sup> a fin de aprovechar las oportunidades que ofrece y promover la acción de los agentes europeos para que estos avances tecnológicos sean útiles en la consecución de nuevos proyectos que beneficien a Europa.

Sin embargo, este no sería tampoco un sistema infalible, contando con ciertas peculiaridades que podrían actuar en contra de exigencias reglamentarias, *“la inmutabilidad y la inalterabilidad que caracterizan a la tecnología Blockchain lo convertirían a priori en una herramienta ideal para dar cumplimiento a algunas de las exigencias que impone la inminente aplicación del RGPD en lo que respecta a la seguridad de los datos y a la reducción de vulnerabilidades. Pero al mismo tiempo, son cada vez más las voces que alertan respecto de la incompatibilidad entre Blockchain y algunas de las previsiones del RGPD”*.<sup>81</sup>

En efecto, ciertas obligaciones establecidas en el RGPD, como la conservación de los datos personales únicamente por el tiempo estrictamente necesario conforme a sus fines, o su modificación, son difícilmente compatibles con el almacenamiento temporalmente indefinido e inalterable de datos que caracteriza el “blockchain”.<sup>82</sup>

Sin embargo, pese a existir varios puntos de conflicto entre el Reglamento y un sistema como el “blockchain”, entiendo que una verdadera protección de datos

---

<sup>80</sup> Comunicado de prensa de la Comisión Europea, “La Comisión Europea pone en marcha el observatorio y foro de la cadena de bloques de la UE”, 2018, disponible en [http://europa.eu/rapid/press-release\\_IP-18-521\\_es.htm](http://europa.eu/rapid/press-release_IP-18-521_es.htm), visitado el 23-03-2019.

<sup>81</sup> POSE VIDAL, M<sup>a</sup> Belén “Blockchain y Reglamento Europeo de Protección de Datos: ¿juntos pero no revueltos?”, (2018), disponible en <http://www.legaltoday.com/practica-juridica/publico/proteccion-de-datos/blockchain-y-reglamento-europeo-de-proteccion-de-datos-juntos-pero-no-revueltos>, visitado el 23-03-2019.

<sup>82</sup> Para un mayor abundamiento en el estudio del “blockchain” en relación con la protección de datos en la Unión: FINCK, Michèle, “Blockchains and Data Protection in the European Union”, *Max Planck Institute for Innovation & Competition Research Paper* N° 18-01, (2017), disponible en <https://ssrn.com/abstract=3080322> o <http://dx.doi.org/10.2139/ssrn.3080322>, visitado el 26-03-2019.

debería conformarse conjuntamente por una normativa a la altura de los riesgos reales y por un sistema informático capaz de hacer frente a los peligros que internet supone respecto a los datos personales. Aunque la tecnología “blockchain” quizás no sea la más apropiada, considero que teniendo en cuenta el sistema actual de internet, la protección efectiva de nuestros derechos debe garantizarse no solo a través de normas bien elaboradas, sino que también debe venir acompañada de una tecnología a la altura, conformando una estructura híbrida, necesaria a fin de consolidar un sistema de protección adecuado a las circunstancias.

Finalmente, en base lo expuesto considero que lejos de establecer una regulación sin defectos, el RGPD es un gran avance en la protección de datos no solo en Europa sino a nivel internacional. Ello ha supuesto que las entidades tanto públicas como privadas realicen un mayor esfuerzo por respetar la normativa, especialmente impulsados por las fuertes sanciones que prevé. Sin embargo, creo que la UE aún cuenta con dos problemas a los que deberá hacer frente si quiere estar en la vanguardia de la protección de datos: las grandes entidades privadas cuyo beneficio reside fuertemente en comerciar con datos personales y el nivel de desprotección que ofrece internet en la actualidad, resultando especialmente difícil salvaguardar la información privada sin una tecnología que respalde a la normativa vigente y permita su amparo efectivo.

## VII. Bibliografía

### A. Legislación

#### Legislación internacional

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950.

Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ETS n.º 108, 28-1-1981.

ONU Asamblea General, Declaración Universal de Derechos Humanos, 10 diciembre 1948, disponible en: <http://www.un.org/es/universal-declaration-human-rights/>, visitado el 01-03-2019.

#### Legislación comunitaria

Tratado de Funcionamiento de la Unión Europea, OJ C 326, 26.10.2012, p. 47–390, disponible en [http://data.europa.eu/eli/treaty/tfeu\\_2012/oj](http://data.europa.eu/eli/treaty/tfeu_2012/oj)

Tratado de la Unión Europea, OJ C 326, 26.10.2012, p. 13–390, disponible en [https://eur-lex.europa.eu/eli/treaty/teu\\_2012/oj](https://eur-lex.europa.eu/eli/treaty/teu_2012/oj)

Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, OJ C 306, 17.12.2007, p. 1–271, disponible en [http://www.europarl.europa.eu/ftu/pdf/es/FTU\\_1.1.5.pdf](http://www.europarl.europa.eu/ftu/pdf/es/FTU_1.1.5.pdf)

Carta de los Derechos Fundamentales de la Unión Europea, OJ C 326, 26.10.2012, p. 391–407, disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012P/TXT&from=ES>

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). OJ L 119, 4.5.2016, p. 1–88.

Directiva 68/151/CEE del Consejo, de 9 de marzo de 1968, Primera Directiva tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades definidas en el segundo párrafo del artículo 58 del Tratado, para proteger los intereses de socios y terceros (DO 1968, L 65, p. 8; EE 17/01, p. 3), en su versión modificada por la Directiva 2003/58/CE del Parlamento Europeo y del Consejo, de 15 de julio de 2003 (DO 2003, L 221, p. 13)

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo OJ L 119, 4.5.2016, p. 89–131

Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos) Bruselas, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), disponible en:

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF>

Resolución 73/22 del Comité de Ministros del Consejo de Europa relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, durante la 224ª reunión de los Delegados de los Ministros, adoptada el 26 de septiembre de 1973.

Resolución 74/29 del Comité de Ministros del Consejo de Europa, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974, durante la 236ª reunión de los Delegados de los Ministros.

Resolución del Parlamento Europeo, sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos – Programa de Estocolmo", de 25 de noviembre de 2009, disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2009-0090+0+DOC+PDF+V0//ES>

Resolución del Parlamento Europeo, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI)), disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES>, visitado el 15-1-2019.

### Legislación nacional

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857, artículo 12.6.

### **B. Jurisprudencia**

Sentencia del Tribunal de Justicia de la Unión Europea de 12 de noviembre de 1969. Erich Stauder contra Stadt Ulm - Sozialamt. Asunto 29-69. ECLI:EU:C:1969:57,

disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A61969CJ0029>, visitado el 13-03-2019.

Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12, Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317.

Sentencia del Tribunal de Justicia de la Unión Europea de 9 de marzo de 2017, asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni ECLI:EU:C:2017:197.

### **C. Publicaciones**

APARICIO VAQUERO, Juan Pablo, “La protección de datos que viene: el nuevo Reglamento General europeo”, *Ars Iuris Salmanticensis Tribuna de actualidad* Vol. 4, (2016), p. 29, disponible en: <http://revistas.usal.es/index.php/ais/article/view/15752>, visitado el 23-01-2019.

Autoritat Catalana de Protecció de Dades en col·laboració amb l'Agència Espanyola de Protecció de Dades i l'Agència Basca de Protecció de Dades, “L'encarregat del tractament en el Reglament General de Protecció de Dades” (RGPD), (2018), disponible en: [http://apdc.gencat.cat/web/.content/03-documentacio/Reglament\\_general\\_de\\_proteccio\\_de\\_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf](http://apdc.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf), visitado el 20-03-2019.

BAIRRAO, Isabel, “Primeras sanciones en aplicación del RGPD en Portugal” *Garrigues digital*, disponible en [https://www.garrigues.com/es\\_ES/garrigues-digital/primeras-sanciones-en-aplicacion-del-rgpd-en-portugal](https://www.garrigues.com/es_ES/garrigues-digital/primeras-sanciones-en-aplicacion-del-rgpd-en-portugal), visitado el 01-04-2019.

BALDUCCI ROMANO, Fabio, “The Right to the Protection of Personal Data: A New Fundamental Right of the European Union”, *SSRN Electronic Journal*, (2013), p. 1, disponible en SSRN: <https://ssrn.com/abstract=2330307>, visitado el 20-11-2018.



BANISAR, David and DAVIES, Simon G., “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments”, John Marshall Journal of Computer & Information Law, Vol. XVIII, (2012), p. 10, disponible en <https://ssrn.com/abstract=2138799>, visitado el 13-03-2019.

BARTOLOMÉ MARTÍN, Antonio, “Sobre el ámbito de aplicación material del reglamento general de protección de datos” Actualidad Jurídica Aranzadi Nº 943, (2018), p. 8, disponible en <https://cms.law/es/ESP/Publication/Bartolome-Martin-sobre-el-ambito-de-aplicacion-material-del-Reglamento-General-de-Proteccion-de-Datos>, visitado el 22-3-2019.

BIURRUN ABAD, Fernando J., “Accountability o responsabilidad activa en el Reglamento General de Protección de Datos”, Actualidad Jurídica Aranzadi Nº 927, (2017), p. 1.

Comisión Europea , comunicado de prensa, “La Comisión Europea pone en marcha el observatorio y foro de la cadena de bloques de la UE”, 2018, disponible en [http://europa.eu/rapid/press-release\\_IP-18-521\\_es.htm](http://europa.eu/rapid/press-release_IP-18-521_es.htm), visitado el 23-03-2019.

Comisión Europea, ¿Qué son los datos personales?, disponible en [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_es](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es), visitado el 09-12-2018.

COOLEY MCINTYRE, Thomas, “A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract” Callaghan, (1879).

Diario ABC, “Escándalo en Nokia: sus teléfonos han enviado información personal de los usuarios a China”, disponible en [https://www.abc.es/tecnologia/moviles/telefonos/abci-escandalo-nokia-telefonos-enviado-informacion-personal-usuarios-china-201903220229\\_noticia.html#vca=mod-lo-mas-](https://www.abc.es/tecnologia/moviles/telefonos/abci-escandalo-nokia-telefonos-enviado-informacion-personal-usuarios-china-201903220229_noticia.html#vca=mod-lo-mas-)

p1&vmc=leido&vso=tecnologia&vli=noticia.foto.tecnologia&vtm\_loMas=si,  
visitado el 29-03-2019

DÍAZ, Efrén, “El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi Doctrinal*, N° 6, (2016), p. 15, disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=5652263>, visitado el 17-11-18.

DOPAZO FRAGUÍO, María Pilar, “La protección de datos en el Derecho Europeo: Principales aportaciones doctrinales y marco regulatorio vigente. (novedades del Reglamento General de Protección de Datos)”, *Revista Española de Derecho Europeo*, N° 68, (2018), p. 138.

DURÁN ARROYO, Alicia “El nuevo reglamento de protección de datos personales. Análisis de su eficacia en la determinación de su ámbito territorial y los remedios en caso de tratamiento ilícito.” *UAM Revista Jurídica Universidad Autónoma de Madrid*, N° 37, (2018), p. 425, disponible en: <https://revistas.uam.es/revistajuridica/article/view/10227>, visitado el 18-12-2018.

EUROPEAN COMMISSION, “First report on the implementation of the Data Protection Directive, (2003), disponible en <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:HTML>, visitado el 11-12-2018.

EUROPEAN COMMISSION, “Special Eurobarometer 431 Data protection”, (2015), disponible en: [https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs\\_431\\_en.pdf](https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf), visitado el 28-12-2018.

FERNÁNDEZ VILLAZÓN, Luis Antonio, “El nuevo Reglamento Europeo de Protección de Datos”, *Foro Nueva época*, vol. 19, N° 1, (2016), p. 401, disponible en <http://dx.doi.org/10.5209/FORO.53399>, visitado el 29-01-2019.

FINCK, Michèle, “Blockchains and Data Protection in the European Union”, Max Planck Institute for Innovation & Competition Research Paper N° 18-01, (2017), disponible en <https://ssrn.com/abstract=3080322> o <http://dx.doi.org/10.2139/ssrn.3080322>, visitado el 26-03-2019.

GÓMEZ BARROSO, José Luis; FEIJÓO, Claudio; MARTÍNEZ, Dolores F.; “Política antes que regulación: la protección de la información personal en la era del big data”, *Economía industrial*, N°. 405, (2017), p. 116, disponible en: <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/GÓMEZ,%20FEIJOO%20Y%20F.%20MARTÍNEZ.pdf>, visitado el 12-12-2018.

HERRÁN ORTIZ, Ana Isabel, “Aproximación al derecho a la protección de datos personales en Europa. El reglamento general de protección de datos a debate” *Revista de Derecho, Empresa y Sociedad (REDS)* N° 8, (2016), p.181, disponible en <https://dialnet.unirioja.es/descarga/articulo/6140105.pdf>, visitado el 11-11-2018

HERRÁN ORTIZ, Ana Isabel, “El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales”, *Dykinson*, p. 2, 2003, extracto disponible en: <http://vlex.com/vid/directiva-frente-libre-circulacion-190765>, visitado el 11-12-2018.

KULK Stefan y ZUIDERVEEN Borgesius, “Google Spain v. González: Did the Court Forget about Freedom of Expression?”, *European Journal of Risk Regulation*, (2014), p.12, disponible en <https://ssrn.com/abstract=2491486>, visitado el 14-02-19.

KUNER, Christopher, “The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law”, *Bloomberg BNA Privacy and Security Law Report*, (2012), pp. 1-15, disponible en [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2162781](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781), visitado el 22-11-2018.

La Vanguardia, “Francia multa con 50 millones a Google” disponible en <https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html>, visitado el 10-04-2019.

MARTÍNEZ LÓPEZ-SÁEZ, Mónica, “Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: la difícil conciliación entre las libertades económicas y la protección de datos personales”, Revista Estudios Deusto, vol. 65/2, (2017), p. 176, disponible en [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwiM\\_\\_ut3pDgAhWfAGMBHeDsDDcQFjAIegQIAhAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6304834.pdf&usq=AOvVaw3AmWhhr4tN3gFxuWuB-7Wu](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwiM__ut3pDgAhWfAGMBHeDsDDcQFjAIegQIAhAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6304834.pdf&usq=AOvVaw3AmWhhr4tN3gFxuWuB-7Wu), visitado el 14-02-19.

MAYOR GÓMEZ, Roberto, “Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)”, Gabilex N° 6, (2016), p. 11, disponible en [http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revisita\\_gabilex\\_no\\_6.\\_autor\\_roberto\\_mayor\\_gomez.pdf](http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revisita_gabilex_no_6._autor_roberto_mayor_gomez.pdf), visitado el 18-12-2018.

MORITZ Marcel y GIBELLO Valentín, “El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro”, Revista de Derecho, N° 27, (2017), p.121, disponible en <http://repositorio.uasb.edu.ec/handle/10644/5948> visitado el 20-11-18.

MINERO ALEJANDRE, Gemma, “Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea”, Anuario Jurídico y Económico Escurialense, N° 50, (2017), p.15, disponible en: <https://dialnet.unirioja.es/descarga/articulo/5876163.pdf>, visitado el 20-11-2018.

PADÍN, Alejandro, “Reglamento General de Protección de Datos de la UE: una visión desde el periodo de adaptación”, Actualidad Jurídica Aranzadi N° 925, (2016), p.2, disponible en [https://www.garrigues.com/es\\_ES/noticia/reglamento-general-de-proteccion-de-datos-de-la-ue-una-vision-desde-el-periodo-de-adaptacion](https://www.garrigues.com/es_ES/noticia/reglamento-general-de-proteccion-de-datos-de-la-ue-una-vision-desde-el-periodo-de-adaptacion), visitado el 29-01-2019.

PANIZA FULLANA, Antonia, “Una nueva era en la privacidad y las comunicaciones electrónicas: la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas”, Revista Doctrinal Aranzadi Civil-Mercantil, N° 7, (2017), p. 1.

PAVÓN PÉREZ, Juan Antonio, “La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales”, Anuario de la Facultad de Derecho, N° 19, (2001), p. 239, disponible en <https://dialnet.unirioja.es/descarga/articulo/831270.pdf>, visitado el 16-04-19.

PÉREZ DE LOS COBOS ORIHUEL, Francisco “El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado”, Unidad Biblioteca de Derecho Comparado, Dirección General de Servicios de Estudios Parlamentarios (DG EPRS) de la Secretaría General del Parlamento Europeo, octubre 2018, [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS\\_STU\(2018\)628261\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf), visitado el 05-04-2019.

POSE VIDAL, M<sup>a</sup> Belén “Blockchain y Reglamento Europeo de Protección de Datos: ¿juntos pero no revueltos?”, (2018), disponible en [http://www.legaltoday.com/practicajuridica/publico/proteccion\\_de\\_datos/blockchain-y-reglamento-europeo-de-proteccion-de-datos-juntos-pero-no-revueltos](http://www.legaltoday.com/practicajuridica/publico/proteccion_de_datos/blockchain-y-reglamento-europeo-de-proteccion-de-datos-juntos-pero-no-revueltos), visitado el 23-03-2019.

REBOLLO DELGADO, Lucrecio, GÓMEZ SÁNCHEZ, Yolanda, “Biomedicina y protección de datos” Dykinson, (2008) p. 23.

SALDAÑA DÍAZ, María Nieves, “El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego”, Teoría y Realidad Constitucional, N° 28, (2011), p. 280, disponible en: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rj>

a&uact=8&ved=2ahUKEwjfk\_HjjObfAhXFRBUIHTXPCvgQFjABegQICBAB&url=https%3A%2F%2Fdialnet.unirioja.es%2Fservlet%2Farticulo%3Fcodigo%3D3883001&usg=AOvVaw2z9cyfK5naWdDCFrncPefe visitado el 23-11-2018.

SARRIÓN J. Esteve, “Las novedades de la nueva normativa de protección de datos y su aplicación a los ensayos clínicos con menores”, Derecho y salud, (Ejemplar dedicado a: XXVI Congreso 2017: Derechos sanitario y ciudadanía europea: los retos), Vol. 27, N° Extra 1, (2017), p. 235, disponible en <https://dialnet.unirioja.es/descarga/articulo/6334698.pdf>, visitado el 28-01-2019.

Sede electrónica de la Agencia Española de Protección de Datos, disponible en <https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/canalesAcceso.jsf>

WARREN, S., & BRANDEIS, L., “The Right to Privacy”, Harvard Law Review, vol. 4 N° 5, (1890), pp.193-220, disponible en [https://www.jstor.org/stable/1321160?seq=1#metadata\\_info\\_tab\\_contents](https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents), visitado el 08-01-2019.