



Universidad
de Alcalá

EL DERECHO AL OLVIDO.

**ESTUDIO DE LA SENTENCIA DEL TJUE *GOOGLE SPAIN*
Y CONSECUENCIAS EN EL ORDENAMIENTO
COMUNITARIO.**

THE RIGHT TO BE FORGOTTEN.

**STUDY OF THE JUDGMENT OF THE CJEU, *GOOGLE
SPAIN* AND CONSEQUENCES IN THE COMMUNITY
LAW.**

Máster Universitario en Acceso a la Profesión de Abogado

Autor: D. BORJA DE BLAS DOMÍNGUEZ.

Tutora: Dra. D^a MONTSERRAT GUZMÁN PECES

Alcalá de Henares, a 14 de febrero de 2017.

RESUMEN

El objetivo de este trabajo consiste en realizar una presentación detallada sobre una de las cuestiones jurídicas que más relevancia ha tenido en el panorama mundial en los últimos años, el derecho al olvido. Para ello haremos un estudio de su concepto y su naturaleza jurídica, así como de sus orígenes y sus características más importantes. En la segunda parte del trabajo nos centraremos en la sentencia que dio origen a este nuevo derecho el llamado caso Google Spain. Y por último analizaremos las consecuencias de esta sentencia y el nuevo reglamento de protección de datos que se creó recientemente en Europa.

PALABRAS CLAVE

Derecho al Olvido, Reglamento UE 2016/679, Google Spain, Directiva 95/46 CE, AEPD, Protección de Datos.

ABSTRACT

The object of this project is make a detailed presentation about one of the most relevant legal issues on the world scene in recent years, “the right to be forgotten”. To that effect, we make a study of it concept and its legal nature as well as of its origins and its most important characteristics. In the second part of the document, we will focus on the judgments that gave rise to this new right called the case Google Spain. Finally, we will analyze the consequences of this sentence and the new regulations of data protection that was created recently in Europe.

KEY WORDS

The right to be forgotten, Regulation EU 2016/679, Google Spain, Directive 95/46 EC, Spanish Data Protection Agency, Data protection

ABREVIATURAS

- ADM: Administración.
- AEPD: Agencia Española de Protección de Datos.
- AH: Antecedente de Hecho.
- AN: Audiencia Nacional.
- AP: Audiencia Provincial.
- ARCO: Derechos de ACCESO, Rectificación, Cancelación y Oposición.
- ART: Artículo.
- ASNEF: Asociación Nacional de Establecimientos Financieros de Crédito.
- CDFUE: Carta de los Derechos Fundamentales de la Unión Europea.
- CE: Constitución Española.
- CEE: Comunidad Económica Europea.
- CENDOJ: Centro de Documentación Judicial.
- CP: Código Penal.
- DPTGSS: Dirección Provincial de la Tesorería General de la Seguridad Social.
- DUDH: Declaración Universal de los Derechos Humanos.
- EEE: Espacio Económico Europeo
- EEUU: Estados Unidos.
- EDIC: Edición
- EDIT: Editorial.
- ETC: Etcétera.
- FECEMD: Federación Española de Marketing Directo y Comercio Electrónico.
- FJ: Fundamento Jurídico.
- INC: Incorporation.
- LLC: Limited Liability Company
- LO: Ley Orgánica.
- LOC CIT: Locus Citatum.
- LOPD: Ley Orgánica de Protección de Datos.
- LOPJ: Ley Orgánica del Poder Judicial.
- LSSI: Ley de Sociedades de Servicios de la Información.
- MF: Ministerio Fiscal.
- MJ: Ministerio de Justicia.
- N^º: Número.

- OP CIT: Opus Citatum
- PÁG: Página.
- PP: Páginas.
- RCP: Registro Central de Penados y Rebeldes.
- RD: Real Decreto.
- RGPD: Reglamento General de Protección de Datos.
- S: Siglo
- SA: Sociedad Anónima.
- SAP: Sentencia de la Audiencia Provincial.
- SAU: Sociedad Anónima Unipersonal
- SEC: Sección.
- SL: Sociedad Limitada.
- SR: Señor
- SS: Seguridad Social.
- STC: Sentencia del Tribunal Constitucional.
- TC: Tribunal Constitucional.
- TD: Tutela de Derecho.
- TEDH: Tribunal Europeo de los Derechos Humanos.
- TFUE: Tratado de Funcionamiento de la Unión Europea.
- TJUE: Tribunal de Justicia de la Unión Europea.
- TS: Tribunal Supremo.
- UE: Unión Europea.
- UNED: Universidad Nacional de Educación a Distancia.
- VID: Vide.
- VVAA: Varios Autores.

ÍNDICE

RESUMEN.....	1
PALABRAS CLAVE.....	1
ABSTRACT.....	1
KEY WORDS.....	1
ABREVIATURAS.....	2
ÍNDICE.....	4
1. INTRODUCCIÓN.....	6
2. EL DERECHO AL OLVIDO.....	7
2.1. CONCEPTO.....	7
2.2. ANTECEDENTES Y FUNDAMENTOS JURÍDICOS DEL DERECHO AL OLVIDO EN LA TRADICIÓN CIVILISTA.....	10
2.2.1. EL PRINCIPIO DE RESPONSABILIDAD CIVIL POR CULPA.....	10
2.2.2. LA REINSERCIÓN SOCIAL DEL DELINCUENTE Y LA CANCELACIÓN DE ANTECEDENTES PENALES.....	12
2.2.3. LA AMNISTÍA.....	13
2.2.4. LA DOCTRINA DE ACCESO A LAS RESOLUCIONES JUDICIALES EN PERSPECTIVA COMPARADA.....	14
2.2.5. LA DIGNIDAD HUMANA Y EL LIBRE DESARROLLO DE LA PERSONALIDAD.....	17
2.2.6. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS Y LA PONDERACIÓN CON LAS LIBERTADES INFROMATIVAS EN INTERNET.....	18
2.2.7. EL DERECHO A LA INTIMIDAD.....	20
2.3. PRESUPUESTOS Y REQUISITOS DEL DERECHO AL OLVIDO.....	21
2.4. LÍMITES DEL DERECHO AL OLVIDO.....	24
3. LA SENTENCIA DEL TJUE DE 13 DE MAYO DE 2014 GOOGLE SPAIN.....	27
3.1. RESOLUCIÓN AEPD.....	28
3.2. CUESTION PREJUDICIAL, CONCLUSIONES DEL ABOGADO GENERAL Y SENTENCIA DEL TJUE.....	39

3.3. ALEGACIONES TRAS LA SENTENCIA DEL TJUE	53
3.4. RESOLUCIÓN DE LA AUDIENCIA NACIONAL.....	55
4. CONSECUENCIAS TRAS LA SENTENCIA DEL TJUE	57
4.1. NUEVO PROTOCOLO DE PROTECCIÓN DE DATOS EN GOOGLE	57
4.2. CAMBIO DE CRITERIO EN LA JURISPRUDENCIA	58
4.3. NUEVA VISION DE LAS AUTORIDADES EUROPEAS	59
4.4. REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS.....	60
5. CONCLUSIONES.....	68
6. BIBLIOGRAFIA	72

1. INTRODUCCIÓN

Hoy en día, internet se ha convertido en un gran foro público por el cual millones de personas navegan a todas horas, todos los días de la semana en busca de información que le haga la vida más sencilla a la par que se expresan y se relacionan con otros internautas.

La red contiene miles de millones de datos, siendo completamente accesibles por cualquiera sin consideraciones espaciales ni temporales. La información personal es una parte muy característica de esta red puesto que permite a los demás usuarios el poder acceder al perfil personal creado específicamente a raíz de los datos que se tienen del propio sujeto, pero no solo afecta los datos personales, sino que este acceso a la información personal nos permite recopilar sus datos históricos con independencia de si se trata de un pasado reciente o uno ha olvidado.

El principal problema de esto es que se proyecta una imagen del individuo que en la mayoría de las ocasiones está desfasada, no siendo adecuada a su realidad actual, ya que como repiten los que ayudaron a crear este mundo digital “Internet nunca olvida”. Es por eso que desde hace un tiempo, la corriente doctrinal más aceptada cree indispensable el poner unos límites a esta capacidad que tiene la propia red de recordar todo, siendo posible así la protección parcial de la intimidad de la persona.

Este trabajo es un recorrido por ese razonamiento, de cómo el derecho al olvido ha pasado a ser la respuesta ante la cada vez más prolífera amenaza contra la intimidad y la dignidad de las personas que puede significar el almacenamiento de datos de forma permanente en la red cuando esos datos conlleva información personal que pueda afectar negativamente a la persona por tratarse de unos datos que produzcan un desajuste entre la realidad actual y los datos publicados en este.

En el primer bloque del trabajo, nos sumergiremos en los preceptos de nuestro ordenamiento civilista que se han ido formando a lo largo del tiempo, los cuales han sido un gran punto de partida para lo que hoy en día se conoce como el Derecho al Olvido en Internet.

Por su parte nos centraremos en los elementos característicos de este nuevo derecho de creación doctrinal, observando sus límites y sus características y viendo cómo afectan al desarrollo de la vida día a día en internet, centrándonos en valorar quien es el encargado del tratamiento de estos datos y que medios proponen los estados y la propia

Unión Europea para ayudar a los particulares en la protección de uno de sus derechos más importantes y a la vez más olvidados en este mundo 2.0.

En el segundo bloque del trabajo estudiaremos la sentencia que dio origen a todo esto, la renombrada sentencia “*Google Spain*”, observando detenidamente sus características, como pasó de ser una reclamación ante la AEPD y se convirtió en una sentencia novedosa que ha cambiado la forma de ver que tenemos de la sociedad hoy en día. Centraremos nuestro estudio en los principales escollos que ha tenido el TJUE para la elaboración de una sentencia que cambió la doctrina que imperaba en Europa y fue el punto de partida para la creación de un derecho que impidiera la comercialización de los datos de carácter personal por parte de las empresas multinacionales.

Observaremos como la AEPD fue pionera a la hora de proteger estos derechos cuando nadie más apostaba por esta forma doctrinal y como esta agencia estatal fue capaz de cambiar la idea que tenían en Europa del derecho a la protección de datos y más concretamente en internet.

Y ya por último veremos las consecuencias directas de este cambio en la doctrina del TJUE en todos los ámbitos relacionados con la protección de datos y como cambio de tal forma el punto de vista que se tenía hasta entonces que no ha quedado más remedio que elaborar un nuevo reglamento de protección de datos que incluyera este nuevo derecho tan importante y tan olvidado.

2. EL DERECHO AL OLVIDO

2.1 CONCEPTO

El derecho al olvido es una creación doctrinal que deriva del derecho fundamental a la libertad informática, que viene dada por la absoluta perennidad de la información en la red y la universalización de todo su contenido, este nuevo derecho actúa como garantía individual frente al tratamiento masivo y descontrolado de los datos personales que se da en Internet.¹ Este nuevo precepto se ha incorporado en el debate de la Unión europea como principal consecuencia de la progresiva exposición del individuo al universo digital

¹ SIMÓN CASTELLANO, P. “El derecho al olvido en internet” en *La libertad de expresión e información en internet*, pág. 452

que permite que se recupere del pasado todo aquello que internet alberga y que dicha información pueda ser vista en el presente en cualquier parte del mundo y que pueda perdurar, siendo accesible, ahora y siempre.²

El problema reside cuando se recupera desde internet una información descontextualizada o prescrita que provoque un daño en la percepción social del sujeto, pudiendo haber sido publicada por el sujeto o con su consentimiento en el pasado, pero que en el momento de su recuperación, puede que sea perjudicial para él.

La libertad informática se ve seriamente afectada por internet ya que no tenemos el control activo de nuestros datos particulares en la red y puede llegar a impedirnos dejar atrás hechos del pasado que pudieran afectar al presente, conectando este derecho con el derecho a la identidad del individuo y al derecho a respetar la propia imagen que se quiere proyectar a la sociedad. Estos derechos, tanto el derecho a la identidad y el derecho a la libertad informática son los principales fundamentos que posee el derecho al olvido.³

El derecho al olvido no se concretaría tan solo en la facultad de supresión de los datos personales y en la oposición a tratamientos de datos ilegítimos, sino que también se tiene que tener muy en cuenta la facultad de evitar que terceros recuerden hechos pasados veraces y que en su día revistieron una notoriedad pública que con el paso del tiempo pereció, imposibilitando reproducir por parte de estos terceros, dichos datos evitando así el perjuicio al individuo.⁴ Este derecho encuentra su contenido en el necesario equilibrio entre la libertad informática el derecho a la identidad y el cumplimiento de las distintas finalidades que se pueden llevar a cabo a través del tratamiento de datos, entre ellas, la finalidad de información. No se trata de una carta blanca para reescribir la propia historia a voluntad del interesado, sino una serie de limitaciones para la perdurabilidad de esa información en internet dando lugar así a los distintos límites y facultades de este nuevo derecho.⁵

Para que este derecho sea efectivo requiere por parte del interesado una acción que derive de su voluntad para que esos datos de carácter personal puedan ser eliminados, ya sea porque se revoca el consentimiento que anteriormente prestó para su utilización,

² *Ídem*

³ GOMES ANDRADE. N.N. “El olvido: el derecho a ser diferente de uno mismo. Una reconsideración del derecho a ser olvidado”, *IDP*, núm. 13, febrero 2012, pág. 75.

⁴ SIMÓN CASTELLANO, P. *Loc cit*, pág. 453

⁵ *Vid.* NOVAL LAMAS, J.J. “Derecho al olvido: algunas consideraciones sobre su futura regulación”, *RCE*, Nº: 120, Octubre-Diciembre 2012, pág.31

porque ya no son necesarios para los fines que fueron concebidos o por otra causa justificada. Esta acción supone una reclamación al responsable del tratamiento de esos datos y este a su vez deberá eliminarlos para que no vuelvan a ser accesibles y desaparezcan de la red impidiendo así la perdurabilidad de estos datos en internet y el efecto que puedan ocasionar en la vida futura del titular.⁶

Por ello, el reconocimiento de éste puede darse con mayor facilidad en países que siguen la tradición jurídica civilista como son España, Francia o Italia. Este reconocimiento no tiene grandes complicaciones a la hora de aplicarse puesto que nuestro sistema así como el de los otros países que comparten nuestra misma visión, es un sistema protector con los datos de carácter personal y siempre tendrán preferencia frente a las libertades que internet implica, sin menoscabar excesivamente las libertades informáticas e informativas.⁷

Sin embargo, no es hasta el año 2016 cuando en nuestro sistema jurídico se introduce una regulación exhaustiva del derecho al olvido, como se recoge en el Reglamento Europeo de Protección de Datos⁸. Con anterioridad, nuestra doctrina así como las autoridades administrativas de protección de datos, la Agencia Española de Protección de Datos (AEPD), supo de la necesidad de introducir una figura jurídica para limitar la intemporalidad de la información que se puede encontrar en internet y que es accesible para todas las personas del mundo.⁹ La propia AEPD dice *“aunque la incorporación inicial de esta información personal a la red “pueda estar legitimada en origen, su mantenimiento universal y secular en Internet puede resultar desproporcionada”*. *Las personas deben disponer de instrumentos de reacción para evitar por su propia iniciativa ser objeto de exhibición global.*”

Así mismo, el Tribunal de Justicia de la Unión Europea (TJUE) dispuso en la sentencia *“Google versus Spain”* de 13 de mayo de 2014¹⁰ que existía un derecho al

⁶ MARTINEZ OTERO, J.M. “El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja”, *UNED. Revista de Derecho Político*, N.º 93, mayo-agosto 2015, pp. 131-133

⁷ SIMÓN CASTELLANO, P. *Loc cit*, pág. 453

⁸ 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)

⁹ *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Declaración sobre buscadores de Internet”, *RAEPD*, 1 de diciembre de 2007, pág. 10.

¹⁰ STJUE/STJCE 13 de mayo 2014, as. C-131/12 *Google Spain S.L., Google Inc. vs. Agencia Española de Protección de Datos*.

olvido derivado de la antigua regulación realizada por la Directiva 95/46, ya derogada¹¹, y los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE), esto supuso el punto de partida para la regulación que existe actualmente y para el derecho al olvido hoy en día.

2.2 ANTECEDENTES Y FUNDAMENTOS JURÍDICOS DEL DERECHO AL OLVIDO EN LA TRADICIÓN CIVILISTA

La tradición civilista, que es la que impera en nuestro país, contiene principios, derechos y valores que son interpretados como auténticos fundamentos o pilares del derecho al olvido digital ya que fueron recogidos por este, pero que imperaban en nuestro ordenamiento jurídico desde hacía mucho tiempo, por lo que este nuevo derecho parte con una ventaja muy significativa a la hora de calar en nuestro sistema jurídico en base a que se va a aprovechar de los dichos antecedentes que forman parte de su estructura, para poder introducirse de forma fehaciente en nuestra sociedad jurídica.

2.2.1 EL PRINCIPIO DE RESPONSABILIDAD CIVIL POR CULPA

La responsabilidad civil extracontractual consiste en la obligación que recae sobre una persona de reparar el daño causado a otro, comúnmente mediante el pago de una indemnización por los perjuicios ocasionados. Esto viene a significar, que el autor ya sea por obra o por omisión tiene que reparar todos aquellos perjuicios en que no exista clara razón o justificación suficiente para que la víctima los soporte por sí sola.¹²

Fue este motivo el cual sirvió de inspiración para la primera referencia jurisprudencial mundial del derecho al olvido. Fue en Quebec en el año 1889, mucho antes de la era digital, cuando un diario local cometió el error de reactivar ciertas

¹¹ 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. Derogada por 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).

¹² DIEZ-PICAZO, L. y GULLÓN, A. *Sistema de Derecho Civil*, Vol. II, Tecnos, 9ª ed., Madrid, 2003, pág. 542.

acusaciones sobre un particular las cuales habían dejado de ser de actualidad muchos años atrás.¹³ El recuerdo de hechos pasados, cuando estos ya no responden a un interés público vigente, puede ocasionar un daño a la vida privada de terceros, naciendo así la responsabilidad civil extracontractual con la conducta de difundir o permitir el acceso masivo a dicha información.¹⁴

En los sistemas jurídicos de tradición civilista, el olvido se presenta como un derecho indirecto, desprendido del derecho a la intimidad o a la propia reputación. Éste se produce después de que se haya distribuido dicha información en un espacio colectivo y tiene como objeto la información que no es secreta, que haya sido compartida y conocida por un grupo de personas. El incumplimiento de la obligación de olvidar comporta la existencia de un deber de olvidar.¹⁵

Ya en España, hasta hace poco los tribunales no habían tenido la oportunidad de conexas el derecho al olvido con la divulgación de hechos del pasado, no fue hasta la sentencia de la AP de Barcelona de 2013¹⁶ cuando se introdujo por primera vez esa conexión en los términos, siendo una sentencia pionera a la hora de vislumbrar esta vertiente del derecho al olvido dentro de la responsabilidad civil extracontractual.

Otro caso que puede establecer las bases de este derecho al olvido, ya en nuestro sistema civilista, es la llamada prescripción adquisitiva o usucapión, que establece el derecho y el deber de olvidar ciertas informaciones del pasado, en este caso la titularidad y posesión de un bien.¹⁷ De alguna manera a través de la prescripción se procura adaptar el derecho al hecho, a la realidad presente, exigiendo que se olvide lo que durante mucho tiempo fue una realidad y se sustituya por otra.¹⁸

¹³ Sentencia *Cour Supérieure du Québec*, caso Goyette c. Rodier (1889)

¹⁴ Vid. SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE*, Bosch, Barcelona 2015, pp. 104-105

¹⁵ TRUDEL, P. “*L’oubli en tant que droit et obligation dans les systèmes juridiques civilistes*”, Traducido por SIMÓN CASTELLANO, P., *El reconocimiento...*, pág. 105.

¹⁶ Sentencia de la Audiencia Provincial de Barcelona (sec. 14) núm. 86/2013, de 8 de febrero de 2013.

¹⁷ OST, F. “El tiempo del derecho” *Siglo XXI editores*, México, 2005, pág. 130.

¹⁸ Vid. SIMÓN CASTELLANO, P., *op cit*, pág. 107.

2.2.2 LA REINSERCIÓN SOCIAL DEL DELINCUENTE Y LA CANCELACIÓN DE LOS ANTECEDENTES PENALES.

Los países que siguen la tradición jurídica civilista, entre ellos España, incorporan en su ordenamiento jurídico una regularización de la prescripción y la cancelación de los antecedentes delictivos, que son pieza clave a la hora de establecer la existencia de los principios fundamentales del derecho al olvido, entendido como la capacidad de volver a empezar sin estar condicionado por los errores del pasado.¹⁹ El derecho al olvido parte del mismo fundamento que la cancelación de antecedentes penales, eso es la idea de que una persona debe tener una segunda oportunidad, estableciéndose un vínculo con la vida privada de los individuos y su personalidad.²⁰

Los reos, una vez puestos en libertad y extinguida su responsabilidad penal, pueden reincorporarse a la sociedad y solicitar la cancelación de sus antecedentes, necesitando previamente un informe del juez que pronunció su sentencia, que haya transcurrido un tiempo aconsejable sin volver a delinquir, en el caso de España, seis meses para penas leves, dos años para penas que no superen los doce meses y los delitos imprudentes, tres años para toda pena inferior a tres años, cinco años para las penas superiores a tres años y diez años para las penas más graves.²¹ Cabe establecer que esta información es custodiada en el Registro Central de Penados y Rebeldes regulado por el RD 95/2009²² y que es el propio Ministerio de Justicia el que tiene que dar autorización para el acceso directo a esta información por parte de algún órgano judicial, cuando estos los reclamen para su utilización en algún procedimiento, así como los interesados. Por lo tanto se puede decir que se vulnera esta garantía y este derecho al olvido en pos de un procedimiento judicial en el que se ha visto implicado el interesado.

De este modo se puede afirmar que el acceso a los antecedentes penales está restringido a terceros, con la excepción del acceso por parte de los Juzgados y Tribunales españoles y del acceso a la elaboración de estadísticas. El RCP se caracteriza por la falta de publicidad de sus inscriptores, los antecedentes penales no son públicos y además los

¹⁹ *Ibíd.*, pág. 108.

²⁰ ARENAS RAMIRO, M. "Hacia un futuro derecho al olvido de ámbito europeo", *La protección de los datos personales en internet ante la innovación tecnológica*, Aranzadi, Cizur Menor, 2013, pp 325-380.

²¹ Artículo 136.1 de Ley Orgánica 10/1995, de 23 de noviembre, del CP.

²² Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia.

datos de carácter personal que contienen están sometidos a la ley de protección de datos²³ pudiendo ser utilizados solamente por el titular, los juzgados y tribunales, determinados cuerpos de la policía, pero después de ser cancelados, solo podían ser utilizados por los juzgados y tribunales.²⁴

2.2.3 LA AMNISTÍA

La figura de la amnistía actúa como una verdadera causa de extinción de la responsabilidad penal, diferenciándola del indulto, que es el perdón en forma de exención del cumplimiento de la pena pero no el olvido del delito ni la desaparición de los antecedentes penales que lleva implícitos. Uno de los claros casos de amnistía en España fue la ley 46/1977²⁵ por la que se amnistió todos los actos de intencionalidad política tipificados como delitos o faltas realizados en España durante la época franquista. En el cuerpo de esta ley establece que la amnistía implica la extinción de la responsabilidad criminal y la eliminación de los antecedentes penales.²⁶ Se entiende que el olvido de los delitos a los que se refiere la ley anteriormente citada no solo es un beneficio para el reo sino que también lo es para la sociedad, responde a un interés general, en este caso la regeneración del régimen político en España.²⁷

Podemos establecer que cuando se produce la amnistía, el delito desaparece, se olvida por parte de la sociedad, aunque eso no es del todo cierto puesto que hoy en día aún se puede reproducir información sobre personas amnistiadas, cosa distinta ocurre en otros países como Francia que existe un derecho al olvido generalizado para temas de amnistía al igual que para los temas de prescripción.²⁸

²³ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

²⁴ GARRIGA DOMÍNGUEZ, A. *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2009, pp 64 y 65

²⁵ Ley 46/1977, de 15 de octubre, de amnistía.

²⁶ Artículo 6 y 7 Ley 46/1977, de 15 de octubre, de amnistía “La amnistía determinará en general la extinción de la responsabilidad criminal derivada de las penas impuestas o que se pudieran imponer con carácter principal o accesorio...”

²⁷ Vid. SIMÓN CASTELLANO, P, *op cit*, pág. 117.

²⁸ *Ibidem*, pp. 119 – 121.

2.2.4 LA DOCTRINA DE ACCESO A LAS RESOLUCIONES JUDICIALES EN PERSPECTIVA COMPARADA

El artículo 18. 4 de la CE²⁹ se crea mucho antes del auge de las nuevas tecnologías, en lo que podemos llamar el inicio de la era de la comunicación. Fue una decisión del legislador a futuro para proteger el honor y la intimidad tanto personal como familiar. Hoy en día se ha convertido en un derecho fundamental, autónomo e independiente introducido en la LOPD y en el RD 1720/2007. Esta modificación del derecho así como el resultado de una globalización absoluta del mundo, han propiciado la aparición en muchos estados del llamado derecho fundamental a la protección de datos, como pasó en España con la LOPD. Esta ley sirve de parapeto ante la exposición continua de datos de carácter personal y el auge de las nuevas tecnologías, en concreto a lo relativo a las resoluciones judiciales.

En los diferentes Estados del planeta se pueden observar diversas formas de garantizar dicho derecho fundamental así como establecer leyes para la publicidad de dichas resoluciones.

En EEUU existe el principio de la *hiperpublicidad* de las sentencias, fuertemente vinculado a la sexta Enmienda constitucional y al derecho a un juicio justo. El principio de *hiperpublicidad* del resultado del proceso está supeditado a la decisión discrecional de los tribunales, permitiendo a los jueces limitar el acceso a los documentos y registros judiciales, estando estos documentos disponibles en internet, con las limitaciones realizadas por los jueces, a un precio definido.³⁰

En Canadá, que sigue en casi todos los aspectos un modelo parecido al estadounidense, en este caso sin embargo, aunque tiene reconocido el derecho de acceso público a los registros judiciales, como su país vecino, su TS estableció que este derecho de publicidad procesal puede prevalecer sobre el derecho de privacidad a menos que pueda haber una exigencia de proteger otro valor jurídico-constitucional que tenga mayor importancia.³¹ Opera así una presunción de acceso público pero pudiendo ser desvirtuada

²⁹ Artículo 18.4 de Constitución Española de 1978. “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”

³⁰ Vid. SIMÓN CASTELLANO, P, *op cit*, pp. 122-126.

³¹ *Caso MacIntyre v Nova Scotia* 1982 SCR 175 a 185.

por cualquier parte procesal que solicite la no divulgación de los documentos judiciales a terceros.³²

En Inglaterra y Gales se comparte la tradición jurídica de los anteriores países reconociéndose el principio de publicidad como regla general, las actas y las pruebas del juicio deben ser aportadas públicamente y no se debe impedir la actividad informativa a menos que los tribunales lo consideren necesario, pero los expedientes judiciales aquí no son considerados de dominio público, no existe un derecho como en los anteriores países a acceder a los archivos y registros de los órganos judiciales. Los archivos y registros penales no son accesibles para el ciudadano al contrario que los civiles, ya que pueden ser útiles de cara a un procedimiento que sea parte un tercero implicado (compraventa, herencia, etc.)³³

Si nos centramos en un estudio más civilista del asunto y olvidamos por un momento la influencia de la *Common Law*, el punto de mira se centraría en Francia, ya que ha mantenido una notable e histórica influencia en el derecho europeo y más concretamente en el español. El acceso a la información procesal (autos, sentencias, títulos ejecutivos) por parte de una de las partes del proceso se recibe a través de su abogado o personándose en el juzgado que la dictó o a través de internet, pero si quien solicita dicha información es un tercero solo podrá acceder a dicha información expresando los motivos legítimos que tiene para acceder a esa información y con la autorización del Ministerio Fiscal.

En 2001 se aprobó una decisión para abordar la difícil tarea de la disociación de los datos de carácter personal de las sentencias, es decir, “*la anonimización*” de los datos de carácter personal, ocultándolos o eliminándolos de la sentencia. En Francia a diferencia de en otros países de la Unión Europea solo se eliminan de las sentencias los nombres personales y las direcciones, lo que le convierte en el país menos garantista de los países civilistas, en lo que se refiere a la protección de datos de carácter personal y a la dignidad humana. En cuanto a la práctica, deja mucho que desear este proceso pues todavía se pueden encontrar en las bases de datos jurídicas francesas nombres propios y direcciones postales de las partes del procedimiento.³⁴

³² Vid. SIMÓN CASTELLANO, P, *op cit*, pp. 127-136

³³ *Ibidem*, pp. 137-140.

³⁴ *Ibidem*, pp. 141-145.

Por otro lado, en Italia se aprecian ciertas similitudes tanto con el sistema francés como con el español. Este sistema está basado en sus inicios en el sistema galo pero ha ido evolucionando gracias a la jurisprudencia hasta formar un sistema único en el mundo. Se ha establecido un modelo acusatorio más propio de la legislación anglosajona en un sistema civilista. En cuanto a la difusión de sentencias y resoluciones, se establece la técnica llamada “*anonimización parcial*”, que consiste en ocultar o eliminar los datos de las personas que intervienen en un procedimiento solo cuando ellas lo exigen o si el tribunal o el juzgado de oficio entienden que es lo más sensato. Queda restringido el acceso al contenido íntegro solo a aquellas personas que demuestren un interés legítimo y solo con la finalidad de dicho interés.³⁵

Por último, en España, en lo relativo a la publicidad de las sentencias o resoluciones judiciales así como los datos personales que están en ellas, debemos observar detenidamente nuestra CE, más en concreto su artículo 120³⁶ desarrollado por el artículo 266 de la LOPJ que permite el acceso a cualquier interesado al texto de las mismas, pero es el artículo 234³⁷ de esta misma ley el que establece funciones a los funcionarios y a los letrados de la administración de justicia para facilitar información acerca del estado de las actuaciones y el artículo 235³⁸ que da la posibilidad de que estos mismos interesados tengan acceso a los libros, archivos o registros judiciales siempre que no tengan un carácter reservado.

Es el TS el que dicta dos condiciones que deben tenerse siempre en cuenta antes de permitir el acceso al texto íntegro de las resoluciones judiciales, la primera, que este acceso no afecte a los derechos fundamentales de las partes del proceso u otros intervinientes en el mismo, con el fin de proteger esencialmente la privacidad y la vida privada, y en segundo lugar, que dicha información obtenida sea de uso meramente judicial no para un beneficio económico a la hora de reutilizar las sentencias, matizando así la figura de persona interesada por la doctrina del TS, instaurando dicha corriente en la legislación actual.³⁹ A consecuencia de esto, se crea el Centro de Documentación

³⁵ *Ibidem*, pp. 145-148.

³⁶ Artículo 120 Constitución Española de 1978. “1. Las actuaciones judiciales serán públicas, con las excepciones que prevean las leyes de procedimiento. 2. El procedimiento será predominantemente oral, sobre todo en materia criminal. 3. Las sentencias serán siempre motivadas y se pronunciarán en audiencia pública.”

³⁷ Artículo 234. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

³⁸ *Ibidem* Artículo 235.

³⁹ *Vid.* SIMÓN CASTELLANO, P, *op cit*, pp. 149-150.

Judicial (CENDOJ), y su esencia recoge perfectamente esos principios, pudiendo acceder a lo que es esencial de forma libre pero no a lo que es accesorio, como los datos personales. Una excepción a esta regla son las sentencias del TC y el TJUE, que se publican íntegramente con los datos personales reales de las partes involucradas en el proceso, llevando a cabo sí una interpretación mucho más laxa del principio a la publicidad judicial que emana de la CE.

2.2.5 LA DIGNIDAD HUMANA Y EL LIBRE DESARROLLO DE LA PERSONALIDAD

Uno de los valores que inspiró la creación de la CE fue el de la dignidad humana y el libre desarrollo de la personalidad, recogido en el artículo 10.1 CE⁴⁰, se entiende que la preinscripción de los antecedentes penales y la llamada “*anonimización*” de las sentencias, son acciones que preservan y protegen este bien jurídico. Este derecho a la dignidad humana viene de la mano de los derechos al honor, la propia imagen, la intimidad y la protección de datos de carácter personal, estando estos “vinculados de forma estricta a la propia personalidad, derivados sin duda alguna de la dignidad de la persona que reconoce el artículo 10 de la CE”⁴¹

De esta manera, el derecho al olvido, que es un derecho creado a partir del precepto constitucional emanado de la dignidad y la libertad, estaría estrechamente ligado a la dignidad humana y al jurisprudencialmente llamado derecho a “*la autodeterminación informativa*”⁴², permitiendo al titular de los datos tener un control efectivo sobre los mismos.⁴³

⁴⁰ Artículo 10.1 CE: “La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.”

⁴¹ STC 231/1988, de 2 de diciembre, FJ 3.

⁴² STC 53/1985, de 11 de abril, FJ 8.

⁴³ *Vid.* SIMÓN CASTELLANO, P, *op cit*, pp. 178-184.

2.2.6 EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS Y LA PONDERACIÓN CON LAS LIBERTADES INFORMATIVAS EN INTERNET

El derecho a la protección de datos constituye uno de los pilares fundamentales para el reconocimiento del derecho al olvido digital. La conexión de los *habeas data*⁴⁴ con la dignidad humana y el libre desarrollo de la personalidad no admite ninguna discusión.⁴⁵ Es el propio TC el que establece que el derecho a la protección de datos es un derecho fundamental autónomo, que podría verse como el poder que tiene toda persona de disponer y controlar sus datos personales frente a terceros, incluyendo las Administraciones Públicas.⁴⁶ La finalidad de este reconocimiento es impedir el uso ilícito y lesivo de esos datos personales para fines comerciales o publicitarios. Es el propio TC el que amplía esa protección no solo a los datos de carácter personal sino a “todos aquellos que sean relevantes o tengan incidencia en el ejercicio de cualquiera de los derecho de la persona, sean o no relativos al honor, la ideología, la intimidad personal y familiar o relativos a cualquier otro bien constitucionalmente amparado por este Tribunal”⁴⁷

Estamos ante un derecho que permite al titular de los datos decidir quién, en qué momento y con qué finalidad va a poder tratar sus datos personales a través del ejercicio propio de este derecho y de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).⁴⁸ En primer lugar, el derecho de Acceso se encuentra regulado en el artículo 15 de LOPD⁴⁹ y en los artículo 27 a 30 del RD 1720/2007. Este derecho permite al ciudadano dirigirse al responsable de un fichero determinado para solicitarle información de sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad de ese tratamiento así como la información del origen de esos datos. En segundo lugar están los derechos de Rectificación y Cancelación, recogidos en el artículo

⁴⁴ “El derecho que asiste a toda persona, identificada o identificable, a solicitar la exhibición de los registros, públicos o privados, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación un mecanismo e instrumento procesal de carácter constitucional que busca tutelar el acceso a la información pública y autodeterminación informativa como medio para acceder, modificar, actualizar y corregir toda información personal o de interés público contenida en registros de entidades públicas y privada” CHANAMÉ ORBE,R., *Habeas Data y el Derecho Fundamental a la Intimidad de la Persona*. Tesis Doctoral (s.p.), Universidad Nacional Mayor de San Marcos, Lima, 2003.

⁴⁵ Vid. SIMÓN CASTELLANO, P, *op cit*, pp. 185 y 186.

⁴⁶ STC 292/2000, de 30 de noviembre. FJ 2 y 3

⁴⁷ STC 292/2000, de 30 de noviembre. FJ 6

⁴⁸ Vid. SIMÓN CASTELLANO, P, *op cit*, pp. 188.

⁴⁹ Artículo 15.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter Personal.

16 LOPD⁵⁰ y en los artículos 31 a 33 del RD 1720/2007. Son las dos opciones que dispone el ciudadano cuando sus datos personales sometidos a tratamiento resultasen inexactos, incompletos o excesivos. El titular de esos datos puede requerir que esos datos se rectifiquen o se cancelen sus datos y se elimine el fichero. El último de los derechos ARCO es el derecho de oposición, regulado en los artículos 34, 35 y 36 del RD 1720/2007⁵¹ concerniente en la facultad que posee el titular de los datos, para dirigirse al responsable del fichero y requerirle que deje de tratar sus datos de carácter personal.

La característica principal de estos derechos, es su carácter personalísimo, es decir que solo pueden ser ejercidos por el titular de los datos o su representante legal o el que voluntariamente designen. El responsable del fichero está obligado a denegar el ejercicio de estos derechos cuando quien lo solicite no sea el titular de los datos o no acredite que actúa en su representación. Otra de estas características es la independencia de estos mismos derechos, es decir que no puede entenderse que el ejercicio de uno de ellos sea un requisito previo para ejercer otro. Por otro lado establecer que la ley obliga al responsable del fichero que alberga dichos datos a facilitar el ejercicio de estos derechos y a dar una respuesta al ciudadano sobre su interés legítimo en estos datos, si esto no fuera así, el titular de estos podría poner una reclamación ante la AEPD que tiene la tutela de estos derechos.⁵²

Todos estos derechos vienen a explicar la facilidad para reconocer el derecho al olvido digital, ya que como bien explica el TC en la sentencia antes citada, “ *el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros[...]* y por tanto, *la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado* ”⁵³

⁵⁰ Artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter Personal.

⁵¹ Artículo 34 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

⁵² ¿Qué son los derechos ARCO? (En línea), <http://www.cuidatusdatos.com/infoderechosarco.html>, (consulta 22 de septiembre de 2016).

⁵³ STC 292/200, de 30 de noviembre, citada anteriormente, FJ 13

2.2.7 DERECHO A LA INTIMIDAD

Como cabe de esperar, no se tuvo una idea de protección de la intimidad, ni siquiera que fuera un derecho inherente al ser humano hasta las revoluciones burguesas de los siglos XVII y XVIII. En la Edad Media, el concepto de intimidad que hoy conocemos no se ajustaba a los parámetros que aquella sociedad exigía para con los suyos, ya que nos estamos moviendo en una sociedad recíprocamente relacionada con fuertes redes comunitarias organizadas de manera estamental. Así, el deseo de estar solo o la aspiración de aislamiento no vendrán a ser realidad sino con el surgimiento político de la burguesía, ya que buscará "*acceder a lo que antes había sido privilegio de unos pocos; aspiración que viene potenciada por las nuevas condiciones de vida. Se concreta en la reivindicación de unas facultades destinadas a salvaguardar un determinado espacio con carácter exclusivo y excluyente*".⁵⁴

Podemos establecer que la idea de intimidad que va ligada a la persona surge del pensamiento burguesita de la propiedad privada. Este derecho intrínseco fue, a raíz de esta época, recogido en todos los escritos jurídicos relacionados con este movimiento, convirtiéndose en uno de los pilares fundamentales para la nueva concepción de la sociedad, y el denominado derecho a estar solo, el germen del derecho a la intimidad, recibió un significativo respaldo de autores influyentes en esa época⁵⁵ como J.S. Mill que sostendrá: "*que sólo se debe responder ante la sociedad por las conductas que afecten a terceros, mientras que en lo que sólo le concierne a él, el individuo no debe responder ante nadie*".⁵⁶

Ya en Estados Unidos, podemos ubicar el origen concreto de la más fiel aproximación a lo que hoy conocemos como derecho a la intimidad, pues fue en un ensayo de Samuel Warren y Louis Brandeis, en 1890, en la revista legal de Harvard donde se asientan los fundamentos del recién creado derecho a la privacidad, entendido como el derecho a estar solo y a ser dejado en paz.⁵⁷ A partir de ahí, la jurisprudencia norteamericana comenzará a prestar auxilio a las demandas fundadas en la protección de

⁵⁴ Vid. PEREZ LUÑO, A. *Derechos Humanos, Estado y Constitución*. Editoriales Tecnos. Madrid, pp. 230-240.

⁵⁵ Vid. UGARTE CATALDO, J.L. "El derecho a la intimidad y la relación laboral" en *Boletín oficial dirección del trabajo*, nº 139/2000, pág. 1

⁵⁶ MILL, J.S. *On Liberty*. En *Prefaces to Liberty*. Bacon Press. Boston. 1959, pág. 251.

⁵⁷ Vid. NOVOA, E. "El Derecho a la Vida y Libertad de Expresión". *Editorial Siglo XXI*. México. Cuarta Edición. México. 1989, pág. 26.

la privacidad, teniendo su hegemonía en el siglo XX, en la Declaración Universal de Derechos Humanos (DUDH), de 1948, que ya habla de vida privada. Entonces este término se recogerá en otros textos legales como la Declaración de Derechos Civiles y Políticos de 1966.

Siendo este antecedente normativo el punto de origen, los países en el período de postguerra comenzarán a incorporar el derecho a la intimidad a sus cartas constitucionales, así por ejemplo ocurrirá con Venezuela (1961), Bolivia (1967), Ecuador (1967), Egipto (1971), España (1978), Chile (1980).⁵⁸ La nota paradójica fue, la llamada “*constitucionalización*” del derecho de intimidad en los países que ya contaban con Carta Magna, que a su vez fueron los que más habían aportado para el desarrollo conceptual de este derecho, como pueden ser EEUU, Alemania, Italia y Francia, que no introdujeron este derecho de lleno en sus constituciones pero que a lo largo del tiempo fue ahondando en su ordenamiento jurídico gracias a la elaboración doctrinaria y jurisprudencial.⁵⁹

2.3 PRESUPUESTOS Y REQUISITOS DEL DERECHO AL OLVIDO

Una vez estudiado de donde viene la idea de establecer una protección a nuestros datos ya sean en internet o en el mundo analógico y como se enfoca el Derecho al olvido en nuestra cultura, pasamos a diseccionar sus elementos. Para estudiar las facultades que otorga el derecho al olvido a sus titulares hay que ver tanto los requisitos como en que supuestos puede existir dicho derecho.

En primer lugar, para que este derecho exista es necesaria la tenencia de datos personales, entendidos estos de forma amplia por el TC en su jurisprudencia⁶⁰ siendo datos personales todos aquellos que permitan identificar al interesado titular de los mismos, desde el nombre y apellidos hasta la dirección IP de un ordenador, fotos ubicaciones, etc. En cambio, en Europa se contempla una doctrina diferente a la que se aplica en España a la hora de establecer que es un dato personal y que no. Ya en el propio RGPD, que estudiaremos más adelante, en su artículo 4 establece que los números de identificación, datos de localización y otros factores específicos no tienen que ser

⁵⁸ Vid. UGARTE CATALDO, J.L. *op cit*, pág. 2

⁵⁹ *Ídem*.

⁶⁰ STC 254/1993, de 20 de julio de 1993 del Tribunal Constitucional; STC 11/1998, de 12 de febrero; y STC 292/2000, de 30 de noviembre.

considerados datos personales en toda circunstancia, no siéndolo cuando no permitan identificar o hacer identificable a una persona.⁶¹

Otro de los presupuestos es la existencia de facultades accesorias como pueden ser la accesibilidad a los datos de carácter personal y la información del tratamiento realizado de estos datos, siendo una pieza clave, ya que sin esta información, el usuario no podrá invocar su derecho al olvido, ya que no sabrá que datos son los que están expuestos ni de qué forma están siendo tratados. Por otro lado, otra de las cualidades para que este derecho al olvido pueda existir es que quien lo ejerza sea una persona física⁶², ya que el titular del derecho nunca podría ser una persona jurídica.⁶³

Por último, cabe destacar la denominada facultad de autocontrol que establece que el mero hecho de ceder tus datos personales al responsable de su tratamiento, ya sea un buscador, una página web, una red social..., no supone la pérdida de la titularidad de estos por parte del interesado y es el responsable del tratamiento el que debe informar al titular sobre dicho tratamiento de los datos y que estos sean accesibles por él⁶⁴. Es un presupuesto indispensable, una premisa básica para entender el derecho a la protección de datos y así mismo el derecho al olvido.

Por otro lado se encuentran los requisitos para poder ejercer dicho derecho al olvido, estos son indispensables para que se pueda comprender este derecho dentro de nuestro ordenamiento jurídico y el de la UE. Pueden cambiar dependiendo de la naturaleza de los datos y de la situación concreta en la que dichos datos están siendo tratados.

Es conveniente empezar por el requisito de la voluntad por parte del titular de los datos, de que desaparezcan de la vida pública, es un proceso consciente y voluntario que no puede ser llevado de oficio, tiene que ser el interesado el que exija que esos datos desaparezcan.⁶⁵ Dichos datos no tienen en un principio más que cumplir la condición de

⁶¹ Artículo 4 REGLAMENTO (UE) 2016/679 (Reglamento general de protección de datos).

⁶² Vid. NOVAL LAMAS, J.J., *loc cit*, pág. 27

⁶³ Considerando 14 Reglamento general de protección de datos: “La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.”

⁶⁴ Vid. VÁZQUEZ DE CASTRO, E., “Protección de datos personales, redes sociales y menores”, *Revista Aranzadi de Derecho y Nuevas Tecnologías (RDNT)*, n.º. 29, mayo-agosto 2012, pág. 38

⁶⁵ TERWANGNE, C. “Privacidad en Internet y el derecho a ser olvidado/derecho al olvido”. *IDP: Revista de Internet, derecho y política*, n.º13, 2012, pág. 60

ser intemporales en Internet y que la facilidad a su acceso pueda menoscabar la propia identidad del titular de los mismos, observando la no necesaria naturaleza privada de estos datos, ya que de ser así, estarían ligados a un derecho de intimidad en la red. Es por ello que el derecho al olvido engloba tanto datos privados como públicos siempre que el acceso a estos mismos pueda suponer un perjuicio para la percepción de su titular y su derecho de dejar atrás la vida pasada. En resumen, el principal requisito del derecho al olvido es que estos datos que se quieren sacar de la esfera pública, transmitan una imagen errónea o no deseada por el interesado, la verificación de un desajuste entre la identidad que transmite la información obsoleta y la que en definitiva, el individuo desea emitir.⁶⁶

Para los datos que no requieren consentimiento para ser tratados, deben darse motivos fundados y legítimos para establecer una oposición a su tratamiento, y conseguir esta supresión mediante el ejercicio del derecho de oposición, sin obviar, que es necesario, tal y como establece el artículo 7f) de la Directiva 95/94/CE, que para este tratamiento, el responsable tiene que tener un interés legítimo y no puede ir en contra de los derechos fundamentales del interesado.⁶⁷ En el caso de que estos datos necesiten consentimiento del titular y este lo haya dado anteriormente, se podrá revocar este consentimiento por el titular siendo así de ejercicio el derecho al olvido. Es importante establecer que dicho consentimiento debe ser inequívoco, no necesariamente expreso, pero que refleje claramente el conocimiento por parte de aquel que lo presta⁶⁸, si el consentimiento lo diera un menor, podrá ser dado libremente a partir de 14 años, los datos de menores de esta edad, deben ser consentidos por sus padres o tutores legales.⁶⁹

Otro de los supuestos sería la caducidad de los datos, para ello, el requisito necesario es que el plazo de conservación autorizado haya expirado y no exista ningún otro fundamento jurídico para que dichos datos sigúan siendo tratados. Por último, los datos recabados para alcanzar un determinado fin, si dejan de ser necesarios para esta meta, podrán ser suprimidos como ya hemos explicado antes a petición del interesado.

Por otro lado, este derecho, como muchos otros, otorga al titular de los datos la posibilidad de solicitar al responsable del tratamiento la supresión o eliminación

⁶⁶ GOMES DE ANDRADE, N.N. *loc cit.*, pág. 74.

⁶⁷ Artículo 7. f 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.

⁶⁸ Artículo 12 del Real Decreto 1720/2007, de 21 de diciembre.

⁶⁹ Artículo 13 del Real Decreto 1720/2007, de 21 de diciembre.

definitiva de los mismos. Esta eliminación habrá de ser completa puesto que no está permitido que quede algún remanente de esos datos en la red, o bien, la limitación de negar el acceso público a esos datos por parte del responsable pero manteniéndolos en su servidor. En algunos casos esta facultad de eliminación se convierte en un derecho a adoptar medidas para hacer anónimo el carácter de los datos, como anteriormente hemos visto que ocurre con las sentencias y demás resoluciones judiciales. Existe también un deber de los responsables del tratamiento de comunicar a terceros que estén utilizando dichos datos de que el titular ha ejercido su derecho al olvido para que dejen de utilizarlos como establece el Reglamento de la UE 2016/679.⁷⁰

Otro de los supuestos que permite este derecho es el poder modificar y rectificar los datos a lo largo del tiempo para que como en el caso de investigaciones o procesamientos, si son absueltos, su nombre no se vea ligado a dicho caso, ya que la justicia determinó que eran inocentes y no modificando esos datos se estaría vulnerando su derecho de inocencia.⁷¹ Esta facultad no se puede establecer dentro del derecho de rectificación comentado en apartados anteriores, puesto que la información en su día era verdad y la información que se ha de publicar es nueva y no pretende rectificar la anterior solo establecer la nueva información más actualizada.

2.4 LÍMITES DEL DERECHO AL OLVIDO.

El derecho al olvido otorga a su titular la cualidad de reescribir su propia biografía, pero no es un derecho absoluto que permita suprimir dichos datos, ya que puede ceder ante intereses constitucionalmente relevantes siempre y cuando el fin sea legítimo y sea respetuoso con el contenido esencial del derecho restringido⁷² Por ello es necesaria la existencia de límites al derecho al olvido, que harán necesario un juicio de ponderación entre el derecho al olvido y aquellos otros derechos o intereses que puedan estar en juego.

⁷⁰ Artículo 17.2 del Reglamento UE 2016/679 de 27 de abril de 2016.

⁷¹ Vid. CASINO RUBIO, M. “El periódico de ayer, el derecho al olvido en Internet y otras noticias”, *Revista española de Derecho Administrativo*, Civitas, nº. 156/2012, pp. 202-213.

⁷² CÓRDOBA CASTROVERDE, D. “El derecho al olvido tras la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014”, en ELDERECHO.COM (En línea), http://www.elderecho.com/tribuna/administrativo/derecho_al_olvido-proteccion_de_datos_11_765430009.html (consulta 26 de septiembre de 2016), pág. 6

Las peticiones de supresión de información relativa a la identidad personal también deben tener en cuenta los intereses que los demás (como colectividad) puedan tener en el mantenimiento de dicha información”. De ahí que los límites al derecho al olvido se encuentren, sobre todo, en derechos que responden a intereses colectivos.⁷³ La necesaria ponderación de estos intereses en conflicto debería hacerse caso por caso y atendiendo a las circunstancias concurrentes, siempre mirando a los pronunciamientos judiciales y de la AEPD, ya que al ser un derecho recién establecido, su concepción está en constante cambio.⁷⁴ Se puede entender como límite la propia existencia de derechos tales como la libertad de expresión y la libertad de información, recogidos en la CE.⁷⁵

El primero de ellos faculta al titular a expresarse libremente en cualquier medio, como por ejemplo Internet, siempre y cuando no se utilicen expresiones vejatorias que, como dice la STC 89/2010, de 15 de noviembre⁷⁶, resulten innecesarias para la exposición de la opinión o juicio de valor. En cambio el segundo es más bien el derecho a la exposición y a la difusión de hechos, tanto de profesionales de la información como de particulares, pero estos han de cumplir en todo caso los requisitos de veracidad e interés público, es en este interés público donde existirá la discusión que en cada caso proceda para establecer que se entiende por tal afirmación.⁷⁷ Como establece el TEDH en la sentencia *Observer and Guardian vs. United Kingdom*, de 26 de noviembre de 1991, “*la prensa ejerce de “perro guardián de la democracia” al difundir ideas y hechos que afectan al interés público, contribuyendo al principio de transparencia y a la necesaria difusión de información veraz.*”⁷⁸

Otro de los límites al derecho al olvido sería el llamado derecho a la memoria, que consiste en la idea de crear una memoria colectiva con todos los datos de internet para su conservación histórica por lo que no se podría “olvidar” ninguno de esos datos. Esta visión resulta excesiva para la mayoría de la doctrina europea ya que requeriría un consentimiento de cesión de datos individualizados a cada uno de los participantes en este derecho. En esta discusión doctrinal se tiene que valorar el derecho a la objetividad entendido como la prohibición del borrado sistemático de datos en ejercicio del derecho al olvido dando así lugar a una opacidad y parcialidad de la información que se encuentra

⁷³ GOMES DE ANDRADE, N.N. *loc cit*, pág. 76.

⁷⁴ CÓRDOBA CASTROVERDE, D. *loc cit*, pág. 6

⁷⁵ Artículo 20.1 a) y d) de CE.

⁷⁶ STC 89/2010 RTC 2010/89

⁷⁷ CÓRDOBA CASTROVERDE, D. *loc cit*, pág. 7

⁷⁸ 26 November 1991, Application No. 13585/88 (European Court of Human Rights)

en internet. Por lo tanto se puede establecer que el verdadero límite a este derecho al olvido es la objetividad de la información.⁷⁹

Por otro lado es preciso apuntar que existe otro límite a este derecho al olvido y es la información con fines históricos, especialmente si se trata de asuntos o hechos relacionados con un personaje público o con acontecimientos políticos, sociales o culturales de gran importancia histórica. Este límite actúa también como propio en el principio de consentimiento del tratamiento de datos personales, ya que se entiende que existe un interés global a la información de una persona o acontecimiento público. Este límite viene expresado en el REPD mencionado anteriormente.⁸⁰

También actúa como límite los fines de investigación científica y estadística, es decir, los datos recogidos que se utilicen para esos fines que no puedan ser tratados de manera anónima dada la naturaleza de la investigación, no podrían ser objeto de este derecho al olvido, *a sensu contrario*, los datos personales que no estén anonimizados pero que no sean necesarios para este trabajo investigador, si deben ocultarse, como es el caso de las sentencias dictadas por los tribunales que se encuentran en las bases de datos de la jurisprudencia⁸¹. Aun cuando esta publicidad de datos sea lícita, se debe instar a ponderar escrupulosamente la relevancia pública de la identidad de las personas afectadas para, en el caso de que no aporte información adicional, evitar la identificación mediante la supresión del nombre e incluso, si fuera necesario, de las iniciales o cualquier referencia suplementaria de la que pueda deducirse la identificación en el caso de que el entorno sea limitado.⁸²

Por último, otros límites legales que, establece la normativa, son los derivados del deber de transparencia y publicidad de las administraciones públicas, directamente ligado con el principio democrático, y del desempeño de la actividad administrativa.⁸³ Es la propia LOPD la que establece que no deberá existir consentimiento y por lo tanto no puede existir derecho al olvido siempre y cuando esos datos personales se recojan por parte de las Administraciones Públicas en el ámbito de sus competencias, convirtiéndose

⁷⁹ GOMES DE ANDRADE, N.N. *loc cit*, pág. 77.

⁸⁰ Artículo 17.1 c) del Reglamento UE 2016/679 de 27 de abril de 2016.

⁸¹ Artículo 9.2 j) del Reglamento UE 2016/679 de 27 de abril de 2016.

⁸² *Vid.* PALACIOS GONZÁLEZ, M. D., “El poder de autodeterminación de los datos personales en internet”, *IDP*, número 14, mayo 2012, pág. 72.

⁸³ GUICHOT, E., “La publicidad de datos personales en Internet por parte de las Administraciones públicas y el derecho al olvido”, *REDA*, núm. 154, 2012, pág. 150.

así en un límite a este derecho, ya que la Administración Pública necesita recabar, tratar y en muchos casos hacer público datos personales de las personas.⁸⁴

3. LA SENTENCIA DEL TJUE DE 13 DE MAYO DE 2014 GOOGLE SPAIN

Este litigio tuvo lugar por la interposición el 5 de marzo de 2010 de una reclamación ante la AEPD contra La Vanguardia Ediciones S.L., *Google Spain* y *Google Inc.* por parte del Sr. Costeja González, de nacionalidad española y con domicilio en España. La reclamación versaba sobre el daño que le estaba ocasionando al usuario la información desfasada que se encontraba en internet utilizando el motor de búsqueda *Google Search*, el cual desplegaba varios vínculos que llevaban a dos páginas del periódico La Vanguardia de 19 de enero y del 9 de marzo de 1998, en las que se podía observar un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social. Estos artículos mencionaban el nombre del Sr. Costeja Gonzalez así como su situación de moroso en la época de los embargos por deudas a la SS de una de sus empresas.

Con esta reclamación lo que el demandante exigía era por un lado que el periódico La Vanguardia eliminase o modificara su publicación de 1998 para que no aparecieran sus datos personales y no se pudiera relacionar esa deuda pasada y ya solventada más que de sobra, con su actual situación financiera y sus actuales negocios y por otro lado, que dicho periódico utilizara las herramientas facilitadas por los motores de búsqueda para proteger dichos datos. Ahora bien, también en dicha reclamación, solicitaba que se exigiera tanto a *Google Spain* como a *Google Inc.* que utilizara su herramienta de buscador para eliminar u ocultar sus datos personales para que a la hora de buscarlos nunca pudieran volver a relacionarse con las publicaciones de La Vanguardia.

Para aclararlo más aún, el Sr. Costeja afirmaba que dicho embargo que se vio sometido en su día estaba completamente solucionado y resuelto hace años y que actualmente no mantenía ninguna relación con esas deuda ni con las empresas que fueron embargadas y que todo esto no hacía nada más que dar publicidad negativa de sus negocios y de él mismo, por un embargo que llevaba solucionado más de 15 años. Para

⁸⁴ Artículo 23.1 e) del Reglamento UE 2016/679 de 27 de abril de 2016.

solucionarlo, el demandante pidió la aplicación del derecho de oposición en virtud de los artículos 6.5⁸⁵ y 30.4⁸⁶ de la LOPD, y el Título II del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Este derecho es la herramienta jurídica que tienen los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.⁸⁷ El demandante invocó este derecho contra *Google Spain* y *Google Inc* por ser la que gestionaba los datos que este no quería que permanecieran en internet.

3.1 RESOLUCIÓN AEPD

En la resolución de la AEPD de día 30 de junio de 2010, se pueden observar varios detalles que pasamos a explicar:

En primer lugar, las alegaciones de Google tienen varios puntos, la primera, el establecer que su filial en España, *Google Spain* no es más que una empresa que da publicidad y que no se puede considerar que todas las búsquedas y los resultados que se efectúen en España tengan como responsable a dicha empresa, puesto que solo y exclusivamente se encarga de publicitar a su empresa matriz, es decir que la responsable principal es *Google Inc*.

[...]Google Spain se limita a representar a Google Inc. en el negocio que ésta desarrolla de vender el espacio publicitario disponible en su página web, es sólo un Agente o representante mercantil exclusivo de Google Inc. y sólo representa a esta

⁸⁵ Art. 6.5 LOPD. “Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.”

⁸⁶ Art. 30.4 LOPD. “Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.”

⁸⁷ Agencia Española de Protección de Datos, Derecho de oposición (en línea), https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposicion-ides-idphp.php, (consulta de 8 de junio de 2016).

*compañía en la promoción de la venta de los servicios publicitarios de Google Inc. Su actividad se limita a dichos servicios y, por ello, ni desarrolla la actividad de buscador ni cabe imputarle ninguna de las actividades ni consecuencias que se deriven de la actividad que ejecuta Google Inc. aunque esta empresa sea la matriz de Google Spain.*⁸⁸

La segunda parte de estas alegaciones está basada en la teoría que se pone de manifiesto en la anterior alegación, que *Google Spain* no tiene responsabilidad jurídica alguna, y solo es responsable *Google Inc.*, que reside en EEUU, no serían aplicables ni la directiva europea de protección de datos ni la ley española que la aplica, solo en este caso serían aplicables las normas de derecho internacional, más concretamente el documento *WP148 del G29*, que establece que los motores de búsqueda no son responsables de los datos de los sitios web proporcionados, que los únicos responsables serían dichos sitios web.

Partiendo de la premisa anterior, esto es, que el responsable único es Google Inc., y tras analizarse en las alegaciones por Google la normativa comunitaria y nacional de transposición, así como los criterios expuestos por el G 29, concluye que “dado que los servicios de buscador los presta Google Inc. Desde los Estados Unidos, no resulta de aplicación ni la directiva europea de protección de datos ni la ley española que la aplica.”

*“El G 29 en su documento WP148 ha puesto de relieve que el motor de búsqueda no puede ser considerado el responsable principal de los datos principales que se tratan, de acuerdo con la legislación europea de protección de datos, sino que este papel principal responsable recae exclusivamente sobre el responsable del sitio web en donde se incluyó la información del interesado”.*⁸⁹

Por otro lado, Google mantiene que no ha habido infracción del derecho de oposición, ya que esta solicitud se mandó contra *Google Spain* y ellos siguen manteniendo que la filial española solo tiene un papel de colaborador para desarrollar el mercado español, que la responsable en todo casi sería *Google Inc.*, a la cual se le remitió dicha petición instando a la cancelación de sus datos de carácter personal de su motor de búsqueda. *Google Inc* por su parte le recondujo otra vez al responsable de la web, el

⁸⁸Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010, pág. 3

⁸⁹ *Idem*

periódico La Vanguardia para que pudiera instar ahí la cancelación de sus datos o en su caso la limitación de los efectos de la publicación con el fin de que los motores de búsqueda no tuvieran acceso a ellos y no pudieran reflejarlos.⁹⁰ Por último, *Google Spain* reconoce que figura en el RGPD como oficina o dependencia ante la que los afectados pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición, pero que su responsabilidad acaba dando traslado a *Google Inc* de dicho expediente.

Frente a la primera alegación de *Google Spain* sobre su comportamiento como filial de *Google Inc* y su nulo tratamiento de los datos de los buscadores, la Agencia se basa en el RD 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LOPD 15/1999, para establecer su posición respecto al tema fundamental de la reclamación. Este RD, establece que se deben regir por estas normas toda entidad cuando el tratamiento de estos datos de carácter personal se efectúe como norma general en las actividades de un establecimiento del responsable del tratamiento, si este se encuentra en territorio español, es decir, que si *Google Spain* en el marco del desarrollo de sus actividades como empresa, está el tratamiento de datos personales aunque sea para otra empresa, en este caso *Google Inc*, al encontrarse la sede de *Google Spain* dentro del territorio español, la ley de aplicación será la ley española, el RD1720/2007.⁹¹

Por otro lado, este mismo artículo establece que si el responsable del tratamiento de datos no está establecido en el territorio de la UE pero sí sigue utilizando medios que están en territorio español para sus tratamientos de datos, salvo que estos sean utilizados como mero tránsito sólo, en los demás casos se debería acoger a las normas españolas, es decir al RD 1720/2007.⁹² En este último caso, siempre la entidad responsable del tratamiento de datos de carácter personal deberá designar un representante en territorio español. En el mismo supuesto, la Directiva 95/46/CE de protección de datos, en su artículo 4 matiza lo ya explicado en el RD 1720/2007 estableciendo que cualquier ente que tenga acceso a datos de carácter personal y los trate, y no esté constituido en un Estado miembro pero sí tenga algún tipo de representante en uno de ellos, como puede ser una

⁹⁰ *Idem*.

⁹¹ Artículo 3.a) de Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

⁹² Artículo 3.c) de Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

filial, deberá aplicar las disposiciones de dicho estado miembro y por ende la de esta directiva.⁹³

La Agencia considera que para evitar que una persona sea excluida de la protección garantizada por esta Directiva, es necesario que todo tratamiento de datos personales efectuado en la CE respete la legislación de uno de sus Estados miembros, que el establecimiento de un ente jurídico en el territorio de un Estado miembro, implica un ejercicio efectivo y real de una actividad como es la instalación de una sucursal o empresa filial con personalidad jurídica.⁹⁴ Que si una empresa tiene varias sucursales o empresas filiales en varios estados miembros, debe garantizar que no se eludan todas y cada una de las leyes de todos los estados miembros en los que tiene sucursal o filial, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades.⁹⁵

Por último considera que el hecho de que el responsable del tratamiento de datos tenga su sede en un tercer país fuera del ámbito de la UE, no puede ser un obstáculo para la protección de las personas de países miembros de la UE, que en estos casos impera la legislación del estado miembro en el que se hayan ubicado los medios utilizados y deben adaptarse garantías con las que se respeten en la práctica los derechos y obligaciones que tiene cada uno de esos ciudadanos.⁹⁶

Para continuar, la Agencia pasa a interpretar los conceptos que establece El documento WP 148 de 4 abril de 2008 elaborado por el Grupo de Trabajo “G 29”, relativo a buscadores. El primero de ellos es concerniente a la calificación que tiene *Google Spain* dentro de *Google Inc* y para con los demás usuarios y Estados. El documento WP 148 establece “*Un proveedor de buscadores que trata datos de los usuarios incluyendo direcciones IP y/ o cookies permanentes que contengan un identificador único se encuentra dentro del ámbito material de la definición de responsable de tratamiento.*” Es por eso que un proveedor de buscadores como puede ser *Google Spain*, que efectúa el tratamiento de millones de datos personales como registros, historiales de búsquedas,

⁹³ Artículo 4 c) Directiva 95/46/CE de Protección de Datos.

⁹⁴ Vid. Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010, pág. 7

⁹⁵ *Ibidem*, pág.8

⁹⁶ *Idem*

debe ser considerado responsable del tratamiento de estos independientemente de las cuestiones relativas a la jurisdicción que puedan aparecer.⁹⁷

Por otro lado, esta resolución establece el derecho nacional aplicable conforme a la Directiva 95/46/CE, *“En el caso de un proveedor de servicios de búsqueda que se establezca y preste todos sus servicios desde uno o más Estados miembros, no existe ninguna duda de que su tratamiento de datos personales se encuentra dentro del ámbito de la Directiva de protección de datos. Es importante hacer constar que en este caso, las normas de protección de datos no se limitan a los interesados situados en el territorio de un Estado miembro o que posean su nacionalidad.”* En el caso de que el proveedor de servicios de búsqueda sea un responsable de tratamiento situado fuera de la CE, existen dos posibilidades. La primera que cuente con un establecimiento en un Estado miembro y que este tratamiento de datos implique a dichos establecimientos, como establecía el artículo 4.1 a) de la Directiva 95/46/CE, *“La existencia de este establecimiento implica el ejercicio real y efectivo de actividades de gestiones estables y debe determinarse con conformidad de la jurisprudencia del TJUE.”*

Así lo establece El documento WP 148 de 4 abril de 2008 elaborado por el Grupo de Trabajo “G 29”, relativo a buscadores. Otro de los requisitos para que se entienda como “establecimiento” es que las operaciones que se realicen deben suponer un papel importante en la operación de dicho tratamientos de datos, es decir, que las actividades realizadas no sean de mero corte secundario, sino que sin ellas, el tratamiento no se podría efectuar.⁹⁸

En segundo lugar, el buscador puede recurrir a medios situados en el territorio de un Estado miembro, debiendo designar un representante en el territorio tal y como establece el artículo 4.1 c en relación con el artículo 4.2 de la Directiva 95/46/CE⁹⁹ Con este artículo se puede entender que el propio ordenador del usuario establecido en el territorio europeo, ya es un medio suficiente como para aplicar el artículo 4.1 c en relación con el 4.2. Es el responsable el que decide tratar los datos personales con este método y se producen diversas operaciones técnicas sin el control del interesado. *“El responsable*

⁹⁷ *Idem*

⁹⁸ *Ibidem*, pp. 9-10.

⁹⁹ Artículo 4.1 c) de la Directiva 95/46/CE.

de tratamiento controla el equipo del usuario y este equipo no se utiliza exclusivamente con fines de tránsito por el territorio de la Comunidad Europea.”¹⁰⁰

La conclusión a la que llega la AEPD conforme al documento WP 148 de 4 abril de 2008 elaborado por el Grupo de Trabajo “G 29”, relativo a buscadores, es que el efecto combinado de los artículos 4.1 a) y c) de la Directiva 95/46/CE de protección de datos se aplica al tratamiento de datos personales por parte de los proveedores de servicios de búsqueda incluso cuando sus oficinas centrales no se encuentren situadas en territorio europeo.¹⁰¹

“En el caso de proveedores de servicios de búsqueda multinacionales:

- Un Estado miembro en el que el proveedor de buscadores está establecido aplicará su legislación nacional en materia de protección de datos al tratamiento, de acuerdo con el artículo 4(1) (a);*
- Si el proveedor de buscadores no se encuentra establecido en ningún Estado miembro, un Estado miembro aplicará su legislación nacional en materia de protección de datos al tratamiento, de acuerdo con el artículo 4 (1) (c), si la empresa recurre a medios, automatizados o no, en el territorio de dicho Estado miembro, con fines de tratamiento de datos personales (por ejemplo, la utilización de una cookie).”¹⁰²*

En el caso de que un proveedor multinacional de buscadores que opere en varios países de la UE, debería cumplir todas las legislaciones en materia de protección de datos, pero un Estado miembro no puede aplicar su derecho nacional a un buscador que en este caso opera en otra legislación del EEE, aunque el buscador recurra a medios en este territorio, en estos casos se aplicará el derecho nacional del Estado miembro que se encuentre establecido el buscador.¹⁰³

¹⁰⁰ Vid. Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010. Págs. 10-11.

¹⁰¹ *Ibidem*, pág. 11

¹⁰² *Idem*.

¹⁰³ Esto se soluciona con el nuevo reglamento (UE) 2016/679 de 27 de abril de 2016 artículo 3 “El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. L 119/32 ES Diario Oficial de la Unión Europea 4.5.2016 2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente

Por otro lado, la AEPD establece que el servicio de búsqueda de GOOGLE utiliza en el tratamiento de datos de carácter personal medios situados en territorio español sin que su utilización sea únicamente con fines de tránsito, ya que en su propia naturaleza, GOOGLE rastrea información de servidores ubicados en todo el mundo incluido en territorio español, los servidores españoles son especialmente rastreados por GOOGLE Spain ya que con ello pueden dar respuestas a las búsquedas de usuarios españoles. “*La información rastreada expresamente por GOOGLE en los servidores ubicados en territorio español incluye datos de carácter personal relativos a personas que no necesariamente son usuarios del buscador y que, al margen de los derechos que debe reconocerse a éstos, también se hallan en disposición de ejercitar sus propios derechos, en relación con los distintos tratamientos que de sus datos realiza GOOGLE.*”¹⁰⁴

También hay que establecer que el servicio de búsqueda que se presta a través de *Google.es* es un servicio de búsqueda especialmente diseñado para los usuarios del territorio español. Todo ello establece que GOOGLE Spain no es sólo un mero instrumento para su empresa matriz, sino que implica un ejercicio real y efectivo de actividades a través de gestiones estables como son estas.¹⁰⁵ Es más, si se tiene en cuenta la LSSI se establece una protección por parte tanto de los medios establecidos fuera del EEE como los de dentro, para con los derechos fundamentales de los ciudadanos.¹⁰⁶

En cuanto se refiere al derecho de cancelación, esta misma Ley establece que los buscadores de internet son servicios de la sociedad de la información, más concretamente servicios de intermediación, por lo que están reglados por las mismas normas que ellos.¹⁰⁷ Una de estas normas es el respeto a la dignidad de la persona como ya establecimos anteriormente, más en concreto la STC 292/200¹⁰⁸ dicta que “*la singularidad del derecho*

de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. 3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.”

¹⁰⁴ Vid. Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010, pp.12-13

¹⁰⁵ *Ibidem*, pp. 14-17

¹⁰⁶ Artículo 8.1.c de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

¹⁰⁷ Anexo apartado b) de la Ley 34/2002 “Servicio de intermediación»: servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.”

¹⁰⁸ STC 292/2000 de 30 de noviembre

a la protección de datos, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de Oct., FJ 4) como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona”.

Ahondando más en el tema, esta sentencia establece “*el artículo 18.4 de la CE contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática”* En cuanto al contenido esencial del derecho a la protección de datos, cabe establecer “*La garantía de la vida privada de la persona y de su reputación posee hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada <<libertad informática>> es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención”.*

Por último entiende el TC que “*El derecho fundamental a la intimidad del artículo 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado”* De esta sentencia se puede extrapolar que la afeción del derecho a la protección de datos atenta o puede atentar al principio de respeto de la dignidad de la persona y esa afectación debe

predicarse de todas y cada una de las garantías que integran el derecho fundamental a la protección de datos personales, entre las que se incluye el derecho de oposición.¹⁰⁹

Por su parte es la propia LSSI la que establece la responsabilidad de los prestadores de servicios, ya que se entiende que dicho prestador tiene el conocimiento efectivo cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada y el prestador “*conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos de los prestadores apliquen en virtud de los acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.*”¹¹⁰ En este caso y tal como establece la propia resolución “*Los datos personales obtenidos por Google afectan a la dignidad de la persona y pueden lesionar derechos de un tercero, por lo que el Director de la AEPD como órgano competente para velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, atendiendo a la reclamación formulada por el reclamante, puede requerir al responsable del tratamiento de los datos, la adopción de medidas necesarias para la adecuación del tratamiento de los datos a las disposiciones de la LO 15/1999, ejerciendo las funciones que le atribuye su artículo 37, así como a los efectos establecidos en los artículos 8 y 17 de la LSSI.*”¹¹¹

A raíz de esto, se debe mencionar el procedimiento TD/266/2007, de Tutela de derechos de la AEPD, el cual establece que “*“Por todo ello, cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación “inconsentida” de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni*

¹⁰⁹ Vid. Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010, pág. 19

¹¹⁰ Artículo 17 de la Ley 34/2002, de 11 de julio

¹¹¹ Vid. Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010 pág. 19

*contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal”.*¹¹²

Por lo que se refiere al fallo, la AEPD estableció:

*“ESTIMAR la reclamación formulada por DON A.A.A. contra GOOGLE SPAIN, S.L. y contra GOOGLE INC., instando a esta entidad para que adopte las medidas necesarias para retirar los datos de su índice e imposibilite el acceso futuro a los mismos”*¹¹³, para llegar a este fallo, se basa en tres puntos:

- Primero: Google Spain actúa como empresa titular en el territorio español y no solo como medio, por lo que la responsabilidad recae en la filial y contra su empresa matriz.
- Por otro lado, basa su fallo en el considerando 45 de la Directiva 95/46/ CE *cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias.*¹¹⁴
- La AEPD aprecia que la ley no establece que los datos personales puedan figurar en los índices que en este caso utiliza Google, no que figuren en las páginas temporales denominadas caché, por lo que *“No existe, por tanto, una disposición legal en contrario respecto del ejercicio del derecho de cancelación frente a Google. Desde Google deberían haberse implementado las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso posterior a los mismos. De acuerdo con lo anterior, procedía la exclusión de los datos personales del reclamante de los índices elaborados*

¹¹² Procedimiento TD/266/2007 en relación con la resolución R/01046/2007

¹¹³ Vid. Resolución nº R/01680/2010 de la AEPD de 30 de junio de 2010, pp. 22-23

¹¹⁴ Ídem.

por Google, por lo que se estima el presente procedimiento de tutela de derechos.”¹¹⁵

“INADMITIR la reclamación formulada por DON A.A.A. contra LA VANGUARDIA EDICIONES, S.L.” en base a que la AEPD entiende que la negación de esta entidad tiene justificación legal ya que *“La publicación de los citados datos se motiva legalmente en la publicación de subastas de inmuebles por la Unidad de Recaudación Ejecutiva, en el presente caso la DPTGSS en Barcelona, cuyo fin pretendido era dar la máxima publicidad a las subastas para conseguir la mayor concurrencia de licitadores.”¹¹⁶* Después de la resolución de la AEPD vista anteriormente, los representantes tanto de Google Inc. Como de Google Spain interpusieron un recurso contencioso-administrativo contra dicha resolución solicitando que se estimase su recurso y se declarara nula o anulable la resolución dictada.¹¹⁷

Dada la complejidad del caso, la AN estimó oportuno elevar una cuestión prejudicial al TJUE, tal y como establece el TFUE¹¹⁸, y dio traslado a cada una de las partes para que alegaran sobre el hecho de hacer esta consulta.

En primer lugar, el Abogado del Estado consideró que la cuestión prejudicial no era necesaria en su vertiente de interpretación, pero en el caso de que se hiciera, realizaría una serie de consideraciones sobre dichas cuestiones a plantear, las cuales no fueron recogidas por la AN. Por su parte, el representante legal del afectado presentó una serie de alegaciones respecto de dicha cuestión prejudicial respecto a la aplicación de la normativa territorial de protección de datos como varias dudas que suscitaba la norma comunitaria. Por último, el representante de Google Spain, consideró que no era necesario el planteamiento de la misma al igual que el representante de Google Inc.¹¹⁹

¹¹⁵ *Ídem.*

¹¹⁶ *Ídem.*

¹¹⁷ Sentencia de la AN 5129/2014 de 29 de diciembre de 2014. AH 1-5

¹¹⁸ Artículo 267 del Tratado de Funcionamiento de la Unión Europea, modificado por el Reglamento 267/2010.

¹¹⁹ Sentencia de la AN 5129/2014 de 29 de diciembre de 2014. AH 6

3.2 CUESTION PREJUDICIAL, CONCLUSIONES DEL ABOGADO GENERAL Y RESOLUCIÓN DEL TJUE

La AN expone una serie de preguntas al TJUE, que en su sentencia de 13 de mayo de 2014 contesta y da pie a un cambio jurisprudencial en el seno de la Unión Europea que ha hecho que se replanteen muchas de las leyes dictadas. A estas preguntas se unen también el gobierno de España, Grecia, Italia, Austria, Polonia y la Comisión Europea. Una vez que se plantean dichas cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea, el Abogado General que fue asignado en este caso, el señor Niilo Jääskinen, elabora una serie de conclusiones de las preguntas emitidas al tribunal para guiar a este sobre su línea a seguir a la hora de contestar a dichas preguntas. Estas conclusiones salen a la luz el 25 de junio de 2013 mucho antes de la contestación del TJUE, y a grandes rasgos estas son sus principales consideraciones.¹²⁰

En primer lugar, en cuanto a los buscadores y prestadores de servicios de la sociedad de información, el Abogado General considera que los motores de búsqueda en Internet no están regulados en la normativa de la UE y más concretamente no estarían sujetos a la Directiva 2000/31/CE, ya que no prestan su servicio como contrapartida de una remuneración por parte de los usuarios de Internet. No entra a valorar el hecho de que la misma directiva incluye expresamente entre los prestadores de servicios de la sociedad de información a los mencionados prestadores de servicios que facilitan instrumentos de búsqueda.

Por su parte, en lo que se refiere al concepto de establecimiento funcional, el Abogado General establece que dicho criterio de establecimiento debe examinarse desde la perspectiva del modelo de negocio, del proveedor de servicios de motor de búsqueda, por lo que propone al TJUE que se aplique la norma europea cuando una empresa que prevé el motor de búsqueda se establece en un Estado miembro, a fines de vender espacios publicitarios en su motor de búsqueda, ya que actúa como intermediaria.¹²¹ También entiende que el motor de búsqueda no puede ser responsable de dicho tratamiento ya que no trata los datos personales que figuran en las webs de terceros con una intención relacionada con sum tratamiento como datos personales, no se realiza de un modo

¹²⁰ CONCLUSIONES DEL ABOGADO GENERAL Sr. NIILLO JÄÄSKINEN presentadas el 25 de junio de 2013

¹²¹ *Ibidem*, pp. 9- 12

sistemáticamente relevante sino como un mero código informático. En todo caso sería responsable de dicho tratamiento si dichos datos estuvieran incluidos en una página web indexada y no respetara los códigos de exclusión de datos de esa página web o si no cumplen la solicitud de esta misma página de no incluir algún dato.¹²²

El Abogado entiende que cuando el motor de búsqueda trata datos personales disponibles en internet en su condición de responsable de tratamiento, la causa de legitimación adecuada es el interés legítimo, es decir, facilitar a los usuarios de internet el acceso a la información, conseguir que la información de internet se difunda de modo más efectivo y poner en marcha diversos servicios de la sociedad de la información proporcionados por el proveedor de servicios del motor e búsqueda en internet subsidiarios respecto al motor de búsqueda.¹²³ Establece que no cabe invocar sin más un derecho al olvido que está por ver, frente a una información publicada legalmente en una página web de un tercero, ya que la directiva reconoce un derecho de rectificación y cancelación de datos debido a su carácter ilegal, falso o incompleto, o un derecho de oposición con razones legítimas propias de sus situación particular ¹²⁴

Dicta que no procede la aplicación de este derecho por tratarse de una publicación obligatoria imperativa por la ley y porque, una preferencia subjetiva por sí sola no equivale a una razón legítima. Por ello, solicitar a los proveedores de servicios de motor de búsqueda que eliminen información que se ha hecho pública por imperativo legal constituiría una injerencia en la libertad de expresión del editor de la página web.¹²⁵ Por ultimo establece que es posible que la responsabilidad secundaria de los proveedores de servicio de motor de búsqueda con arreglo al Derecho nacional implique la existencia de deberes que exijan bloquear el acceso a páginas web de terceros con contenidos ilegales, como las páginas web que vulneran derechos de propiedad intelectual o que muestran información injuriosa o delictiva¹²⁶

Una vez visto las conclusiones del Abogado General, tenemos que hacer un ejercicio de retrospección para poder estudiar individualmente cada pregunta formulada por la AN.

¹²² *Ibidem*, pp. 12-15

¹²³ *Ibidem*, pp. 17-20

¹²⁴ *Ibidem*, pp. 20-25

¹²⁵ *Ibidem*, pp. 26-30

¹²⁶ *Ibidem*, pp. 30-36

En primer lugar, la AN pregunta:

1. Por lo que respecta a la aplicación territorial de la Directiva 95/46/CE y, consiguientemente de la normativa española de protección de datos:

a) ¿Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la Directiva 95/46/CE, cuando concurra alguno o algunos de los siguientes supuestos:

- Cuando la empresa proveedora del motor de búsqueda crea en un Estado Miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese Estado.*
- cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa.*
- cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria?*

Conforme a esta primera pregunta, el Tribunal establece que aunque no está probado que Google Spain realice una actividad vinculada al almacenamiento de datos o información para Google Inc¹²⁷, sí se ha podido demostrar que tiene una actividad de promoción y publicidad en territorio español y que constituye una parte esencial de la actividad comercial del grupo empresarial y está estrechamente vinculada a los buscadores de Google.¹²⁸ EL tribunal entiende que concuerdan los requisitos del considerando 19 de la Directiva¹²⁹, ya que entiende a Google Spain como una filial de Google Inc, que tiene personalidad jurídica propia y que opera en territorio español, por lo que se le puede catalogar como establecimiento como apunta el artículo 4 de la

¹²⁷ Google Inc y Google Spain sostienen que la actividad de este último es meramente publicitaria en el territorio español que opera, no tiene otra función que la de publicitar el buscador.

¹²⁸ STJUE de 13 de mayo de 2014, asunto C-131/12 § 46

¹²⁹ Considerando 19 de la Directiva 95/46.

directiva 95/46¹³⁰ No obstante, para cumplir el requisito del artículo anterior, es necesario que el tratamiento de esos datos de carácter personal por parte del responsable “*se lleve a cabo en el marco de las actividades*” de un establecimiento situado en territorio de un Estado miembro.¹³¹

El tribunal constituye¹³² que no es necesario que dicho tratamiento sea efectuado “*por*” el propio establecimiento, sino que se realice “*en el marco de las actividades*” de este¹³³ no pudiendo se resta expresión objeto de una interpretación restrictiva ya que desea garantizar una protección completa y eficaz y la propia jurisprudencia del TJUE así lo establece.¹³⁴ Es más, de la propia directiva 95/46 ¹³⁵se desprende que el legislador pretendió evitar que una persona quedara excluida de dicha protección y que las empresas pudieran eludir dicha protección, estableciendo un ámbito de aplicación territorial muy extenso. Por todo ello, el tribunal considera que el tratamiento de datos de carácter personal que se realiza a través de un motor de búsqueda como en este caso Google Search, que está gestionado por una empresa con domicilio en un Estado tercero fuera de la UE, pero que dispone de un establecimiento en un Estado miembro como es el caso de Google Spain, se efectúa como establece la Directiva 95/46 en el marco de las actividades de dicho establecimiento, ya que, este está destinado a la promoción y venta en el Estado miembro de los espacios publicitarios del motor de búsqueda, que rentabilizan el servicio de dicho motor.

Tanto las actividades del gestor del motor de búsqueda como las de su establecimiento situado en el Estado miembro están estrechamente ligadas, ya que es la única forma de que el motor de búsqueda sea rentable.¹³⁶ Así mismo matiza el tribunal que la mera presentación de datos personales en una página como resultado de una búsqueda constituye un tratamiento de dichos datos y que a su vez si estos datos están acompañados de publicidad, se está incurriendo en un tratamiento de datos personales controvertidos en el marco de la actividad publicitaria y comercial del establecimiento

¹³⁰ Artículo 4.1 a) de la Directiva 95/46.

¹³¹ Aquí Google Spain y Google Inc. Niegan que éste sea el caso, dado que el tratamiento de datos personales controvertido en el litigio principal lo lleva a cabo exclusivamente Google Inc., que gestiona Google Search sin ninguna intervención por parte de Google Spain, cuya actividad se limita a prestar apoyo a la actividad publicitaria del grupo Google, que es distinta de su servicio de motor de búsqueda.

¹³² Esta tesis es la que acoge la AEPD y el Gobierno Español.

¹³³ STJUE de 13 de mayo de 2014, asunto C-131/12 § 52

¹³⁴ STJUE de 12 de julio de 2011, asunto C-324/09 L'Oréal y otros contra Ebay Internacional AG y otros.

¹³⁵ Considerando 18 de la Directiva 95/46.

¹³⁶ STJUE de 13 de mayo de 2014, asunto C-131/12 § 55-56

del responsable, este es el caso concreto que ocurre con Google Spain cuando actúa como establecimiento publicitario y a su vez de tratamientos de datos de su empresa matriz Google Inc.¹³⁷

De todo esto debe desprenderse que el TJUE responde a la primera pregunta apartado a) interpretando el artículo 4.1a) de la mencionada directiva, en el sentido de que se lleva a cabo un tratamiento de datos de carácter personal en el “*marco de las actividades*” de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, entendiendo que si el gestor de un motor de búsqueda en este caso Google Inc crea en un Estado miembro una sucursal o filial como es Google Spain, y su destinación es garantizar la promoción y la venta de espacios publicitarios a propuesta de dicho motor y esta actividad la dirige a los habitantes del estado miembro está actuando como un establecimiento del motor de búsqueda, y que esas actividades de publicidad aparecen en la misma búsqueda que los datos personales, se debe entender que la actividad de esta empresa es la de gestionar dichos datos.¹³⁸

En segundo lugar la AN pregunta:

- b) *¿Debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un "recurso a medios situados en el territorio de dicho Estado miembro" cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro?*
- c) *¿Puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet? Si la respuesta a esta última cuestión fuera afirmativa, ¿puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas?*
- d) *Con independencia de la respuesta a las preguntas anteriores y especialmente en el caso en que se considerase por el Tribunal de Justicia de la Unión que no*

¹³⁷ *Ibidem*, § 57

¹³⁸ *Ibidem*, § 60

concurren los criterios de conexión previstos en el art. 4 de la Directiva, ¿Debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea?

El TJUE aprecia que como ya se ha pronunciado sobre la letra a) de la primera de las cuestiones y sobre todo dadas sus observaciones, no es necesario pronunciarse sobre los siguientes apartados que confeccionan la cuestión primera, de tal forma que da por finalizada dicha cuestión para dedicarse a las demás.¹³⁹

A continuación la AN expone su segunda pregunta con varios apartados, los dos primeros, se complementan, por eso el TJUE decide contestarlos a la vez.

2. Por lo que respecta a la actividad de los buscadores como proveedor de contenidos en relación con la Directiva 95/46/CE de Protección de Datos:

2.1. En relación con la actividad del buscador de la empresa "Google" en internet, como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos" contenido en el art. 2.b de la Directiva 95/46/CE?

2.2. En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita: ¿Debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la empresa que gestiona el buscador "Google" es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?

La opinión que da Google Spain y Google Inc sobre este tema es que la actividad de los motores de búsqueda no puede considerarse tratamiento de datos personales que se muestran en las páginas web de terceros que ellos presentan en la lista de resultados, dado que ellos tratan la información globalmente sin discriminar entre datos personales y el resto de la información, pero aun que la actividad se pueda clasificar como un tratamiento

¹³⁹ *Ibidem*, § 61

de datos, queda muy claro que ellos se desvinculan diciendo que no se considerarían responsables de este tratamiento ya que ellos no conocen los datos y no pueden ejercer un control sobre ellos.¹⁴⁰ Por su parte, el señor Costeja, y los demás gobiernos de los países implicados sostienen que dicha actividad implica claramente un tratamiento de datos, distinto al que tienen los editores de los sitios web pero sigue siendo un tratamiento de datos ya que el determina la finalidad y los medios para dicho tratamiento.¹⁴¹

El Tribunal dictamina que como ya ha tenido la ocasión de declarar¹⁴², la conducta que consiste en hacer referencia en un sitio web a datos de carácter personal se debe considerar en toda su plenitud un tratamiento de datos, correspondiendo con la definición que establece la directiva 95/46 en su articulado.¹⁴³ Es más, el tribunal establece que dada la naturaleza del buscador que utiliza la información que encuentra en internet para recogerla, extraerla, registrarla y conservarla en sus servidores y con eso facilitar el acceso a esa información a los usuarios en forma de listas de resultados, está llevando a cabo punto por punto las operaciones descritas en el artículo anteriormente citado conllevando por ello a ser calificadas dichas operaciones como parte de un tratamiento de datos, sin ser relevante que el gestor del motor realice a su vez las mismas operaciones con otro tipo de información y no distinga entre esta última y los datos personales, aun habiendo sido estos ya publicados en la red.¹⁴⁴ El TJUE también declara que dicho tratamiento es igual de efectivo y se basa en los mismos preceptos aunque la información tratada ya estuviera publicada y en circulación en Internet, ya que se entiende que la mera recepción y organización de la información que ya existe, es una parte más del tratamiento de datos, como la reiterada jurisprudencia del tribunal así lo considera¹⁴⁵

En cuanto a la responsabilidad que tiene el gestor de búsqueda del tratamiento de los datos personales, gestionados en el marco de una actividad de búsqueda, el TJUE considera que es el gestor el que determina los fines y los medios de la actividad y que por consiguiente debe considerarse responsable de dicho tratamiento en virtud del artículo

¹⁴⁰ *Ibidem*, § 22

¹⁴¹ *Ibidem*, § 23-24

¹⁴² Sentencia *Lindqvist* C- 101/01, apartado 25

¹⁴³ Artículo 2b) de la Directiva 95/46. “tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.”

¹⁴⁴ *Ibidem*, § 28-29

¹⁴⁵ Sentencia *Satakunnan Markkinapörssi y Satamedia*, C- 73/07 apartados 48 y 49

2 d) del artículo anteriormente mencionado¹⁴⁶ De esto cabe distinguir dos posiciones, la primera es la del gestor de búsqueda que como ha quedado acreditado por el tribunal, es responsable del tratamiento de esos datos aun cuando no los distingue de la información global, y la segunda la de los editores de los sitios web donde consta la información, que hacen que esos datos figuren en sus dominios web y se añaden a los gestores de búsquedas. Es lógico asegurar que sin la ayuda en la difusión masiva por parte de esos gestores de búsqueda, la información que aparece en los sitios web sería muy difícil de encontrar, y sobre todo que la utilización de estos motores de búsqueda hacen posible la búsqueda por parte de un internauta común del nombre del interesado, ofreciéndole una organización y un fácil acceso a su información ofreciendo una visión estructurada de toda la información que puede hallarse en internet sobre la persona investigada, permitiendo así que se pueda establecer un perfil del interesado.¹⁴⁷ Es decir, el tribunal establece que como consecuencia de la afección que puede resultar de la actividad del motor de búsqueda a la de los editores de sitios web, a los derechos fundamentales de respeto a la vida privada y a la protección de datos personales, es el propio gestor el que debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicha actividad satisfaga las exigencias de la directiva antes mencionada para que pueda surtir efectos sus garantías y se lleve a cabo una protección eficaz y completa del derecho al respeto a la vida privada de los afectados.¹⁴⁸

Ya por ultimo han de detallarse que aunque los editores de sitios web tiene la facultad de indicar a los gestores de búsqueda que información desean excluir total o parcialmente de los índices, no quita que la falta de tal indicación libere al gestor de las responsabilidades por el tratamiento de estos datos, no modifica el hecho de que el gestor es quien determina los fines y los medios del tratamiento, y la falta de exclusión por parte de los gestores de sitios web de esos datos personales no elimina la responsabilidad del gestor que dicta el artículo 2 de la directiva antes mencionada.¹⁴⁹

¹⁴⁶ Artículo 2d) de la Directiva 95/46 “responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos ,personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario”

¹⁴⁷ STJUE de 13 de mayo de 2014, asunto C-131/12 § 35 – 37.

¹⁴⁸ *Ibidem*, §38

¹⁴⁹ *Ibidem*, § 39-40

Por todo ello el Tribunal responde a esta segunda pregunta letras a) y b) con el artículo 2 b) y d) de la directiva 95/46, interpretándolo de tal marea que por un lado “*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 el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales*” y por otro lado que “*el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del mencionado artículo 2, letra d).*”¹⁵⁰

A continuación el TJUE analiza los dos últimos apartados de la segunda pregunta.

2.3 En el caso de que la respuesta anterior fuera afirmativa: ¿Puede la autoridad nacional de control de datos (en este caso la Agencia Española de Protección de Datos), tutelando los derechos contenidos en el art. 12.b) y 14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa "Google" para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?.

2. 4 En el caso de que la respuesta a esta última pregunta fuera afirmativa, ¿Se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen?

En este caso Google Spain y Google Inc consideran que se debería aplicar el principio de proporcionalidad y que cualquier solicitud de eliminación de información debe dirigirse al sitio web que la tenga, ya que considera que este asume la responsabilidad de publicar dicha información, y que imponer que se retire de sus índices información publicada en internet vulnera los derechos fundamentales de los editores de sitios web y del resto de internautas y hasta los del propio gestor.

Por otro lado, el gobierno austriaco se desmarca de los demás considerando que solo se podría ordenar el borrado de esos ficheros al gestor del motor de búsqueda si se ha declarado la ilegalidad o inexactitud de esos datos o si se ha ejercido por parte del interesado su derecho de oposición y ha resultado exitoso. Los demás gobiernos, el señor

¹⁵⁰ *Ibidem*, § 41

Costeja y la Comisión Europea consideran que se puede ordenar directamente al gestor de un motor de búsqueda la retirada de esos datos de sus índices y memoria interna sin dirigirse previamente o de manera simultánea al editor de la página web en la que se ha publicado dicha información. El caso de que la información sea lícita y siga figurando en la web, carece de relevancia para ellos, ya que estiman que las obligaciones de dicho gestor van por encima de la licitud o no de la información. En este punto el gobierno polaco discrepa y cree que si la información es, lícita y todavía sigue en funcionamiento, el gestor estaría liberado.¹⁵¹

En primer lugar el TJUE hace referencia al espíritu de la norma, en este caso de la Directiva 95/46,¹⁵² dado su estudio, el Tribunal puede decir que esta norma tiene por objeto una garantía elevada de protección de las libertades y los derechos fundamentales de las personas físicas con una especial mención a la protección de la vida privada en relación con este tratamiento de datos personales.¹⁵³ Esta protección tiene su máxima expresión en las obligaciones que incumben a las personas que efectúan dichos tratamientos, como pueden ser la calidad de los datos, seguridad técnica, notificación a las autoridades del control y las circunstancias en las que se efectúa el tratamiento y por otro lado en los derechos otorgados a las personas cuyos datos hayan sido objeto de tratamiento de ser informadas acerca de este tratamiento, de poder acceder a esos datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias.¹⁵⁴

El tribunal estima que como ya ha declarado en reiterada jurisprudencia,¹⁵⁵ cualquier tratamiento de datos personales que pueda atentar contra los derechos y las libertades fundamentales de los individuos, en particular el derecho a la intimidad y a la vida privada, va en contra de los principios generales del Derecho cuyo respeto lo garantiza el Tribunal y que están recogidos en la Carta de derechos fundamentales de la Unión Europea¹⁵⁶. Es la propia Carta la que establece que toda persona tiene el derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.¹⁵⁷ Se entiende

¹⁵¹ *Ibidem*, §63-65

¹⁵² Considerando 10 de la Directiva 95/46.

¹⁵³ *Vid.* Sentencia IPI, EU:C:2013:715, apartado 28

¹⁵⁴ Considerando 25 de la Directiva 95/46

¹⁵⁵ Sentencias *Connolly/Comisión*, C-274/99 P, EU: C: 2001:127, apartado 37 y Sentencia *Österreichischer Rundfunk* y otros, EU: C: 2003:294, apartado 68.

¹⁵⁶ Artículo 7 Carta de Derechos Fundamentales de la UE “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.”

¹⁵⁷ Artículo 8 Carta de Derechos Fundamentales de la UE

que todo tratamiento de datos debe ser conforme a los principios relativos a la calidad de datos¹⁵⁸ y con alguno de los principios relativos a la legitimación del tratamiento de datos¹⁵⁹ como reitera el propio tribunal en su jurisprudencia.¹⁶⁰ La propia directiva establece en el artículo anteriormente citado que se permite el tratamiento de datos de carácter personal cuando es necesario para la satisfacción del interés legítimo perseguido por el responsable o por terceros a los que se le comuniquen los datos pero prevaleciendo siempre el interés y los derechos y libertades fundamentales del interesado.¹⁶¹ Se precisa una ponderación de los derechos e intereses en liza pero se han de tener en cuenta los derechos del interesado vistos anteriormente en la CDHUE.¹⁶²

Por su parte el artículo 14¹⁶³ de esta misma directiva da un poder al interesado para oponerse al tratamiento de sus datos personales salvo cuando la legislación nacional disponga otra cosa, en este caso la ponderación que ha de efectuarse, permite tener en cuenta de un modo más claro y específico todas las circunstancias que han rodeado a la situación del interesado, y el tratamiento no podría referirse ya a esos datos.¹⁶⁴ El interesado puede dirigir esa solicitud directamente al responsable del tratamiento que le debe poner fin. Si no accediese a esa solicitud, se podría ir directamente a las autoridades de control o tribunales para que ordenen las medidas precisas en consecuencia.¹⁶⁵

A este respecto, como ya se ha señalado anteriormente, este tratamiento de datos puede afectar significativamente al interesado, ya que con la mera introducción de su nombre en el motor de búsqueda, se puede hallar una lista detallada de datos de carácter personal que le pertenecen, y como establece la jurisprudencia del TJUE, *“el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo”*¹⁶⁶ El tribunal estipula que el mero interés económico del gestor no le desvincula de las responsabilidades derivadas del tratamiento de datos, y aunque sí es verdad que la

¹⁵⁸ Artículo 6 de la Directiva 95/46.

¹⁵⁹ Artículo 7 de la Directiva 95/46

¹⁶⁰ Sentencia *Österreichischer Rundfunk* y otros, EU:C:2003:294, apartado 65; Sentencia ASNEF y FECEMD, C-468/10 y C-469/10, EU:C:2011:777, apartado 26 y *Worten*, C-342/12, EU:C:2013:355, apartado 33

¹⁶¹ STJUE de 13 de mayo de 2014, asunto C-131/12 § 73-74.

¹⁶² Sentencia ASNEF y FECEMD, EU: C: 2011:777, apartados 38 y 40.

¹⁶³ Artículo 14 Directiva 95/46.

¹⁶⁴ STJUE de 13 de mayo de 2014, asunto C-131/12 §76.

¹⁶⁵ Artículo 28 de la directiva 95/46.

¹⁶⁶ Sentencia *eDate Advertising* y otros, C-509/09 y C-161/10, EU:C:2011:685, apartado 45

supresión de dicha información podría repercutir en el interés legítimo de los internautas para con esa información habría que buscar un justo equilibrio entre los derechos de ambas partes, dependiendo de la naturaleza de la información, de la persona afectada y del interés del público que puede variar según la función que esta persona desempeñe en la vida pública.¹⁶⁷

Por otro lado el Tribunal aclara que no es necesaria la eliminación de forma simultánea o posterior de los datos de carácter personal del motor de búsqueda y del sitio web, ya que los motores de búsqueda son los responsables de su difusión global por la red y el propio Tribunal señala que sería imposible imponer esa eliminación a los responsables del sitio web dada la facilidad de copia que se tiene en internet y que muchos de estos no están sujetos al derecho de la unión, por lo que no se podría llevar una protección eficaz y completa del interesado.¹⁶⁸

Otro de los motivos de la no regulación de esta imposición a los editores de páginas web dentro de la directiva europea es que su fin puede ser un fin exclusivamente periodístico y se benefician del artículo 9 de la misma, que versa sobre la libertad de expresión y el tratamiento de datos ligado a esta,¹⁶⁹ mientras que este no es el caso de los motores de búsqueda, por lo que los derechos que puede ejercitar el interesado son sobre los gestores de los motores de búsqueda y no sobre los sitios web¹⁷⁰, ya que *“los intereses legítimos que justifican estos tratamientos pueden ser diferentes, y, por otro, las consecuencias de estos tratamientos sobre el interesado, y, en particular, sobre su vida privada, no son necesariamente las mismas.”*¹⁷¹ *“puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página web.”*¹⁷²

Por todo ello, el Tribunal decide contestar a este grupo de preguntas con los artículos 12 y 14 de la Directiva 95/46, interpretándolos en el sentido de que siempre que se cumplan los requisitos de estos artículos, los gestores de motores de búsqueda están obligados a eliminar de la lista de sus resultados dados a partir del nombre de una persona, vínculos a páginas web de terceros y que contiene datos de carácter personal aun no

¹⁶⁷ STJUE de 13 de mayo de 2014, asunto C-131/12 § 80-81

¹⁶⁸ *Ibidem*, § 82-84.

¹⁶⁹ Artículo 9 de la Directiva 95/46.

¹⁷⁰ STJUE de 13 de mayo de 2014, asunto C-131/12 § 85

¹⁷¹ *Ibidem*, §86

¹⁷² *Ibidem*, §87

habiéndose borrado simultáneamente o con posterioridad esos datos de las páginas web referidas o aun cuando la información fuese lícita.¹⁷³

Ya por último se le plantea al Tribunal la tercera pregunta:

3. Respecto al alcance del derecho de cancelación y/oposición en relación con el derecho al olvido se plantea la siguiente pregunta:

3.1. ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarlo o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"

Sobre esta última pregunta, tanto Google Spain, Google Inc en conjunto con los Gobiernos de Grecia, Austria y Polonia y la Comisión Europea estiman que la respuesta debe ser negativa, pero existen dos claras posiciones dentro de esta negativa. En primer lugar la posición que adoptan Google Spain, Google Inc., el gobierno de Polonia y la Comisión que a este respecto establecen que en los anteriormente citados artículos 12b) y 14 de la Directiva 95/46 confieren un derecho al interesado únicamente si el tratamiento controvertido va en contra de la Directiva o por razones legítimas personales y no por el simple hecho de que el particular considere que la información le perjudica o solo que no quiere que esos datos permanezcan. Y por otro lado están los gobiernos de Grecia y Austria que consideran que en este caso, el interesado debe dirigirse al editor del sitio web.¹⁷⁴

En contraposición a esta tesis se encuentran las ideas del Sr. Costeja, el gobierno de España y el de Italia, que entiende que el interesado puede oponerse a la indexación de sus datos de carácter personal por el motor de búsqueda si la difusión de estos datos por el trabajo de este le perjudica y que los derechos de protección de dichos datos personales y el respeto a la vida privada, es decir el derecho al olvido, prevalecerían sobre los intereses del gestor y el interés general de la libertad de información.¹⁷⁵

¹⁷³ *Ibidem*, §88

¹⁷⁴ *Ibidem*, § 90

¹⁷⁵ *Ibidem*, § 91

Como ya ha reiterado el tribunal en este caso, la incompatibilidad de estos datos con la directiva no exige que estos sean incorrectos, bastaría que fueran inadecuados, no pertinentes y excesivos de los fines del tratamiento, que no estén actualizados o de que se conserven en un periodo superior a lo necesario, por lo que si los datos incluidos en la lista de resultados, que aparecen tras la inclusión del nombre del interesado, que hacen referencia a sitios web, tiene alguna de las características antes mencionadas, se estaría actuando en contra de la directiva a habida cuenta del conjunto de circunstancias que caracterizan el caso en concreto, por lo que deberían eliminarse.¹⁷⁶ El Tribunal establece que se tendrán que efectuar valoraciones y examinar los casos concretos para decidir si el derecho a la intimidad de la persona afectada, puede prevalecer sobre los derechos económicos del buscador y sobre todo, sobre los derechos que tienen los demás usuarios de este a la información que estos datos arrojan. En el caso concreto que nos ocupa y siendo estos datos personales relativos a un embargo por deuda a la Seguridad Social y no siendo el Señor Costeja una persona de especial relevancia en la vida pública, el Tribunal entiende que estos datos después de haber pasado más de 16 años desde que ocurrieran los hechos, podrían llegar a ser perjudiciales para su persona, por lo que se deberían poder eliminar del buscador sin mayor problema.¹⁷⁷

Por todo ello, el Tribunal decide contestar a esta última pregunta que se debe examinar si el interesado puede tener derecho a que estos datos de carácter personal no estén vinculados a la búsqueda de su nombre a través de un buscador. Como la Carta de los derechos fundamentales de la Unión Europea establece que los interesados pueden solicitar que su información no esté a disposición del público en general se entiende que4 estos derechos prevalecen sobre el interés económico del motor de búsqueda y sobre el posible interés que pueda tener el público en acceder a la mencionada información, pero aquí recalca el Tribunal que el papel que desempeña el interesado en la vida pública es muy importante ya que si es un papel relevante, esta injerencia estaría justificada por el interés preponderante de dicho público a tener acceso a la información de que se trate.¹⁷⁸

¹⁷⁶ *Ibidem*, § 92-94.

¹⁷⁷ *Ibidem*, § 95-99.

¹⁷⁸ *Ibidem*, § 99.

3.3 ALEGACIONES TRAS LA SENTENCIA DEL TJUE.

Una vez resueltas las cuestiones prejudiciales presentadas por la Audiencia Nacional, se dan traslado a los interesados para que puedan presentar alegaciones a estas respuestas y en general a la sentencia emitida por el TJUE, estas alegaciones son recogidas por la misma sentencia de la AN.

En primer lugar el representante de Google Spain alega que existe una falta de legitimación pasiva en el procedimiento administrativo previo a la resolución de la AEPD, ya que aunque en la sentencia del TJUE se haya dicho que Google Spain es el responsable del tratamiento, sigue siendo una filial de Google Inc. y por tanto es la que gestiona el motor de búsqueda y quien podría ser obligada a eliminar dichos resultados, tal y como se deduce de actuaciones anteriores de la AEPD¹⁷⁹ por otro lado, alega también la falta de motivación de la resolución recurrida, ya que no lleva a cabo “*la ponderación de los derechos en conflicto exigida por la doctrina establecida en la Sentencia del TJUE.*”¹⁸⁰ Dice Google Spain que esto le causa indefensión ya que la AEPD no ha valorado si este tratamiento de datos personales es o no compatible con la directiva 95/46 o si simplemente, la solicitud del interesado estaba debidamente justificada. Otra de las alegaciones vertidas por Google Spain es la infracción de las libertades de información y de expresión que a su juicio, el bloquear una página web podría ir en contra de estos derechos, es más en el caso concreto del bloqueo de esa publicación de la Vanguardia, establecen que existen más noticias en la misma página que si podrían ser interesantes para el público, como la noticia de un debate parlamentario e informes de un juicio contra la banda terrorista ETA. Ellos establecen que el motor de búsqueda no puede determinar si una información es relevante o no para el público y depender de ese criterio para bloquear o no los sitios web, con esto lo que dicen es que la resolución lesiona la libertad de expresión e Google Inc.¹⁸¹ Por último, Google Spain considera que la sentencia del TJUE no ampara la retirada y el bloqueo del acceso futuro a unos datos, sino que no se muestren enlaces concretos entre los resultados cuando la búsqueda sea específicamente con el nombre del interesado, y que la AEPD lo que quiere es poder controlar el resultado

¹⁷⁹ Aquí se refiere a la resolución de 18 de diciembre de 2013 contra Google Inc, que en ese momento estaba recurrida ante la AN. Entiende Google Inc. que por analogía la única responsable frente a los tribunales españoles es la empresa matriz.

¹⁸⁰ Sentencia de la sala de lo contencioso de la Audiencia Nacional de 29 de diciembre de 2014. FJ 5.1 a)

¹⁸¹ Sentencia de la sala de lo contencioso de la Audiencia Nacional de 29 de diciembre de 2014. FJ 5.1 c)

de las búsquedas algo prohibido en la directiva 2000/31/CE¹⁸² y declarado contrario a derecho por los tribunales españoles.¹⁸³

El representante de Google Inc. establece como su filial que la resolución impugnada carece de la motivación que exige la sentencia del TJUE, se establece que la AEPD no ha llevado a cabo ningún juicio de valor entre los distintos derechos enfrentados, entre el derecho de protección de datos del interesado y las libertades de información y expresión y el interés público de los usuarios de Google.¹⁸⁴ Y por otro lado estipula que las páginas web a las que se hay pedido a Google que elimine los enlaces, tienen más información que se manifiesta como de relevancia pública. Por su parte Google Inc entiende que si se llegase a bloquear estos enlaces *“infringiría las libertades de expresión e información tanto de los Editores de las informaciones como de los usuarios del buscador interesados en acceder a esa información.”*¹⁸⁵ Se aduce también a la libertad de empresa recogida en la Carta de los Derechos Fundamentales¹⁸⁶ y en la Constitución Española¹⁸⁷, ya que la medida que restringe estos derechos fundamentales adoptada por la AEPD la consideran demasiado restrictiva para el fin perseguido. Por último Google Inc estipula que la sentencia del TJUE no ampara la resolución de la AEPD en lo de retirar datos e imposibilitar el acceso futuro a los mismos, entiende que lo que dice el Tribunal es que cuando la petición de solicitante sea pertinente se puede ordenar que no se muestren enlaces concretos entre los resultados cuando se busque específicamente el nombre del afectado.¹⁸⁸

El Estado español aduce que la sentencia del TJUE confirma íntegramente la resolución de la AEPD, se resuelven las cuestiones de competencia territorial y de legitimación pasiva al incluir a Google Spain con resultado positivo para la AEPD, reconociéndose la legitimidad pasiva de este último por tener una actividad de gestión publicitaria y estar unida de forma indisoluble a su matriz, permitiendo así tener la competencia territorial dentro del territorio español. Por otro lado, la sentencia del TJUE

¹⁸² Artículo 15 de Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

¹⁸³ Sentencia de la Audiencia Provincial de Madrid de 14 de enero de 2014. Asunto Gestevisión Telecinco, S.A. y Telecinco Cinema, S.A.U. contra YouTube LLC.

¹⁸⁴ Sentencia de la sala de lo contencioso de la Audiencia Nacional de 29 de diciembre de 2014. FJ 5. 2 a)

¹⁸⁵ *Ibidem*, fJ 5. 2 b)

¹⁸⁶ Artículo 16 de la Carta de Derechos Fundamentales de la Unión Europea.

¹⁸⁷ Artículo 38 de la Constitución Española de 1978.

¹⁸⁸ Sentencia de la sala de lo contencioso de la Audiencia Nacional de 29 de diciembre de 2014, fJ 5. 2 d)

señala la posibilidad de que un particular pueda dirigirse ante la entidad que trata los datos y pedir su cancelación si dirigirse a la fuente de información. La misma sentencia estipula que la solicitud de que determinada información no se incluya en los índices del buscador no vulnera el derecho a la información puesto que se conserva la información original pero lo que se modifica es el tratamiento que afecta a la intimidad. Y por último, El estado Español cree que la sentencia del TJUE marca un antes y un después pues aborda la existencia del derecho al olvido, haciendo una ponderación directa de la situación entre el interés particular del afectado y su derecho a la intimidad contra el interés del buscador y el interés de la colectividad y su derecho a la información.

Para esto el TJUE da su receta en forma de reglas precisas: *“No es preciso que la información contenida en el tratamiento de datos cause un perjuicio al interesado; el derecho a la intimidad del interesado prevalece, en todo caso, al interés económico del buscador; y la intimidad del afectado prevalece al interés público en general de acceder a la información excepto cuando por razones concretas deba reconocerse que existe un interés preponderante del público en acceder a la información, como en los casos en que el interesado tenga un papel importante en la vida pública.”*¹⁸⁹

El representante del Sr. Costeja tal y como considera el Estado español, entiende que ha quedado de manifiesto que Google Spain es el responsable en España del tratamiento de datos y por tanto se tiene que adaptar a las leyes españolas y a los tribunales tanto españoles como europeos. Entiende también que como el buscador no tenía un derecho equivalente al que posee el diario la Vanguardia, es decir derecho a la libertad de prensa y derecho la información, se ha producido una transmisión de datos la cual es susceptible de recurrir. Por ultimo cree que la configuración que hace el TJUE sobre el derecho al olvido hace que prevalezca la vida privada del individuo frente al interés económico del motor o frente al interés público de encontrar esa información.¹⁹⁰

3.4 RESOLUCIÓN DE LA AUDIENCIA NACIONAL

En primer lugar, la AN trata el tema de la actividad del motor de búsqueda haciendo referencia a lo pronunciado por la sentencia del TJUE, que establece que Google

¹⁸⁹ *Ibidem*, fj. 5.3

¹⁹⁰ *Ibidem*, fj. 5.4

Spain es el responsable del tratamiento de los datos en España por estar estrechamente ligada su función publicitaria y de soporte con el tratamiento de datos efectuado.¹⁹¹ En otro de los fundamentos jurídicos aborda el tema de la aplicación territorial de la norma, la cual establece que por ser Google Spain el representante legal de Google en España y por ser parte activa en las actividades de tratamiento de datos de carácter personal, se debe aplicar la normativa conforme a la protección de datos de España.¹⁹²

En cuanto a la falta de motivación de la resolución de la AEPD, la AN establece que si es verdad que la resolución impugnada tiene como defecto un aclara falta de motivación y de ponderación entre los derechos de libertad de información y de interés público y los derechos de intimidad y el derecho al olvido pero tal y como establece la AN, estas alegaciones se deberían haber establecido en los escritos de demanda¹⁹³ tal y como establece la ley de jurisdicción contencioso administrativa.¹⁹⁴

Por otro lado, la AN desestima este motivo de impugnación al considerar que Google Spain tiene la legitimación pasiva necesaria para responder de sus actos ante el tribunal al igual que desestima la alegación de que la resolución tiene un objetivo imposible de obrar por parte de Google Spain.¹⁹⁵ En cuanto a la indefensión alegada por Google, la AN entiende que se han seguido todos los trámites necesarios en este procedimiento y que nunca se ha ido claramente en contra de una de las partes y que los aludidos han estado siempre debidamente representados no siendo viable la alegación de indefensión por parte de estos.¹⁹⁶

Por su parte, la AN en cuanto a la alegación de vulneración de la libertad de empresa, establece que si bien es verdad que existe tal derecho, la sentencia del TJUE nunca lo ha vulnerado, sino que lo ha ponderado con los otros derechos con los que entraba en conflicto y se ha visto como esta libertad de empresa debe ceder ante el derecho a la intimidad como ante la protección de datos y el derecho al olvido.¹⁹⁷ De lo establecido por la AN se debe entender que el derecho a la libertad de expresión queda salvaguardado en el sitio web de inicio, que es el que tiene la potestad de ejercitar dicho derecho, lo que si se discute y debe valorarse es el derecho que tienen los internautas a encontrar la

¹⁹¹ *Ibidem*, fj. 6

¹⁹² *Ibidem*, fj.7

¹⁹³ *Ibidem*, fj.8

¹⁹⁴ Artículo 65. 1 de Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

¹⁹⁵ *Ibidem*, fj.9

¹⁹⁶ *Ibidem*, fj.10

¹⁹⁷ *Ibidem*, fj.11

información relacionada, el llamado interés público, pero la AN cree que debe prevalecer el derecho a la protección de datos en ese caso.¹⁹⁸ Por todo ello, la AN desestima los recursos tanto de Google Inc, como de Google Spain contra la resolución de la AEPD y estimar la reclamación de Sr. Costeja en materia de tutela de derechos.¹⁹⁹

4. CONSECUENCIAS TRAS LA SENTENCIA DEL TJUE

4.1 NUEVO PROTOCOLO DE PROTECCIÓN DE DATOS EN GOOGLE.

Tras la sentencia del TJUE y la posterior aclaración y fallo de la AN, los representantes de Google Spain y Google Inc establecieron que el ejercicio de ponderación al cual obliga este tribunal supondría un coste demasiado elevado, y se podría incurrir en una sobreprotección de todos los datos. Frente a esta indeterminación a la hora de aplicar o no hacerlos, estos criterios a la hora de saber si la información que se está tratando es susceptible de ser un dato de carácter personal perjudicial para el individuo, Google decidió designar un Consejo Asesor integrado por diez miembros presididos por el máximo responsable de la compañía el señor Eric Schmidt, que son los encargados de establecer los criterios que sirven para sopesar caso por caso, individualmente, la aplicación del derecho al olvido del individuo frente al derecho a la información del público.²⁰⁰

Este Consejo realizó una ronda de contactos con expertos económicos, tecnológicos, jurista, etc., con el único fin de identificar los temas más controvertidos en relación a la ponderación de estos derechos.²⁰¹ Este grupo de trabajo ha querido establecer unos criterios de ponderación a la hora de enfrentar ambos derechos destacando entre ellos, si la búsqueda es a partir del nombre del individuo o bien a partir de un seudónimo; ponderar la vida pública del afectado; la exactitud de los datos; la necesidad de estos con los fines perseguidos; si estos datos son sensibles afectando a la religión, sexualidad, política, etc.; contextualización de los mismos; si se pone al titular en una situación de riesgo; si se produce daño a este; si están relacionados con delitos penales; si los datos están publicados en los boletines oficiales; o en las hemerotecas digitales. Todas estas

¹⁹⁸ *Ibidem*, f.12

¹⁹⁹ *Ibidem*, fallo.

²⁰⁰ <https://www.google.com/advisorycouncil/> fecha de consulta 15 de noviembre de 2016.

²⁰¹ Las reuniones fueron en Madrid, Roma, Paris, Varsovia, Berlin, Londres y Bruselas en 2014 <https://www.google.com/advisorycouncil/>

cuestiones tendrían que ser valoradas a la hora de establecer la ponderación y si es o no receptivo la supresión del índice del buscador dichos resultados.²⁰²

4.2 CAMBIO DE CRITERIO EN LA JURISPRUDENCIA.

Como cabe de esperar una sentencia tan sonada como la del TJUE, ha tenido repercusión en la jurisprudencia de toda Europa, centrándonos en España, los tribunales han aceptado de muy buen grado la incursión de este nuevo derecho al olvido en nuestro ordenamiento jurídico, siendo así, que la propia sentencia de la AN que dio paso a la sentencia del TJUE, ya habla abiertamente de derecho al olvido digital.²⁰³

En otro caso, la sentencia de la AP de Barcelona 364/2014, reconoce también el derecho al olvido en España y lo liga indisolublemente a la protección de datos de carácter personal, pudiendo ejercitar sus derechos de cancelación y oposición de esos datos. Lo novedoso de esta sentencia lo podemos encontrar en su fallo, el cual condena a Google a pagar una indemnización por la vulneración de dicho derecho, esta Audiencia reconoce el derecho del afectado a percibir una indemnización económica en la medida que se ha producido un incumplimiento del responsable del tratamiento, en este caso Google y que como consecuencia de esto, se ha ocasionado un dolo o perjuicio indemnizable.²⁰⁴ La propia sentencia distingue entre la protección administrativa de del derecho a la protección de datos, que corresponde a la AEPD y al protección judicial que puede obtenerse de los juzgados civiles y en la que se incluye una reclamación por los daños ocasionados.²⁰⁵ La citada sentencia de la AP de Barcelona es la primera sentencia europea que incorpora los pronunciamientos de la sentencia del TJUE, seguido de esta, el Tribunal de Gran Instancia de París dictó otra sentencia que conforme a la doctrina del TJUE, obligaba a Google a suprimir los enlaces que hacían referencia a dos personas y al pago de una indemnización por daños y perjuicios.²⁰⁶

Con esto se observa como los juzgados y tribunales de los distintos Estados miembros, en este caso españoles, empezaron a aplicar la doctrina del TJUE poco después de su pronunciamiento considerando que la normativa europea sobre protección de datos

²⁰² Vid, SIMÓN CASTELLANO, P. *op cit*, pp 270-272.

²⁰³ *Ibidem*, pág. 272.

²⁰⁴ Sentencia nº 364/2014 de AP Barcelona, sección 16ª, 17 de julio de 2014. Fallo.

²⁰⁵ Simón Castellano, P. *op cit*, pág. 173.

²⁰⁶ Sentencia del Tribunal de Gran Instancia de París de 16 de septiembre de 2014.

personales se aplica al buscador y que éste al enlazar realiza un tratamiento de datos personales. Estos dos preceptos permiten que los tribunales de los Estados miembros puedan canalizar los daños y perjuicios de esta exposición de datos personales en los buscadores y poder así condenarles a pagar una indemnización.²⁰⁷

Por otro lado, más recientemente, se encuentra la sentencia del TS de 15 de octubre de 2015²⁰⁸ pronunciándose por primera vez en Europa sobre el alcance de este nuevo derecho. Como estipula el TS refiriéndose sobre todo a los periódicos digitales *“la vinculación entre los datos personales de una persona y una información lesiva para su honor e intimidad en una consulta por Internet va perdiendo su justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esas personas, carecen de interés histórico. Por ello, el derecho a la protección de datos personales justifica que, a petición de los afectados, los responsables de las hemerotecas digitales deban adoptar medidas tecnológicas impedir que en sus páginas la información obsoleta y gravemente perjudicial pueda ser indexada por los buscadores de Internet.”*²⁰⁹

4.3 NUEVA VISIÓN DE LAS AUTORIDADES EUROPEAS.

La AEPD publicó una nota de prensa donde valoraba muy positivamente la sentencia del TJUE y daba a conocer su satisfacción al ver reconocidas sus tesis en relación con los buscadores y el derecho al olvido en internet. Tanto la AEPD como sus homólogas europeas se reunieron en junio de 2014 para analizar las consecuencias de dicha sentencia y comenzar a identificar los elementos relevantes para construir una posición común. Con este propósito hablaron con los principales buscadores de internet y con los medios de comunicación, y han creado una red específica al efecto para registrar las decisiones adoptadas por las autoridades de control de la UE para permitirles identificar casos similares o supuestos especialmente complejos.

Por su parte la Comisión Europea ha manifestado su satisfacción por la sentencia del TJUE ya que ellos propusieron la regularización del derecho al olvido mucho antes

²⁰⁷ *Ibidem*, pp. 274-275.

²⁰⁸ STS de 15 de octubre de 2015. 545/2015.

²⁰⁹ *Ídem*.

de que el Tribunal se pronunciara. Resaltan que esta sentencia no crea un “*superderecho*” que se encumbra sobre los demás.²¹⁰

4.4 EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS.

En 2016 se da vigencia al nuevo Reglamento Europeo de Protección de Datos, que viene a sustituir a la Directiva 95/46, y que recoge muchos de los aspectos fundamentales de la jurisprudencia del TJUE sobre el derecho al olvido. Desde su artículo 1º, este nuevo reglamento ha querido reforzar la protección de los datos de carácter personal de las personas físicas en el ámbito de la UE desde una perspectiva más integradora y coherente motivado por lo expuesto en su exposición de motivos.²¹¹ Una de las cosas que viene bien resaltar es la incesante consolidación del principio de la libre circulación de los datos personales entre los Estados miembros, evitando que se restrinjan por motivos relacionados con la protección y el tratamiento de datos personales.²¹²

En cuanto al ámbito de aplicación material, el propio reglamento establece uno de los aspectos esenciales de éste, y es que se aplicará a los tratamientos totales o parcialmente automatizados de datos de carácter personal, así como al tratamiento no automatizado de estos datos con el fin de ser incluidos en un fichero, haciendo clara referencia a los *index* utilizados por buscadores como Google, que acaparan toda la información de los sitios web para tratarla y hacer listas de resultados²¹³. Por su parte, en este mismo artículo se establecen las excepciones para las cuales no se aplicará dicho reglamento sino que se recurrirá o bien al reglamento 45/2001 o bien a la directiva 2001/31/CE²¹⁴

Una de las claras diferencias que dicta este nuevo RGPD frente a su predecesora la Directiva 95/46 es su artículo 3 donde aparece referido el ámbito territorial de aplicación. Esta diferencia esencial se explica como consecuencia de la unificación resultante de la adopción de las normas en el RGPD, en la anterior directiva, el capítulo abordaba el derecho nacional aplicable para los casos concretos de la directiva, en cambio

²¹⁰ ÁLVAREZ RIGAUDIAS, C. “Sentencia Google Spain y Derecho al Olvido” en *Actualidad Jurídica Uría Menéndez* 2015, pp 110-118.

²¹¹ Considerando 4 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.

²¹² Artículo 1 del Reglamento (UE) 2016/679

²¹³ Artículo 2.1 RGPD.

²¹⁴ Artículo 2.2 y ss. RGPD.

con el nuevo Reglamento, pasa a denominarse ámbito territorial, pierde importancia la determinación de la legislación de qué Estado miembro es aplicable en materia de protección de datos personales.²¹⁵ Ambas normas coinciden en algo fundamental, en la determinación del ámbito espacial de aplicación de esta legislación europea. Si bien la Directiva cumplía dicha función ya que determinaba el ámbito territorial de las legislaciones nacionales de transposición, el nuevo Reglamento se refiere al alcance territorial de las normas de éste. La trascendencia de esta función y la importancia de estas normas están vinculadas con las diferencias que existen en materia de protección de datos a nivel mundial entre los estándares de tutela personales y el elevado nivel que ostenta en esta materia la proteccionista legislación europea.²¹⁶

El nuevo artículo 3 del RGPD, parte de la semejanza de su homólogo anterior, el artículo 4.1 de la Directiva 95/46 siendo iguales a la hora de partir desde una clasificación “*tripartita*” y previendo como el primer criterio determinante del sometimiento a la legislación europea el que el tratamiento de datos personales ha de tener lugar en el marco de las actividades de un establecimiento del responsable o del encargado en la Unión. Por otro lado se contempla como criterio alternativo, que si el responsable esté establecido en un lugar en que el Derecho de los Estados miembros es de aplicación en virtud del derecho internacional, también se debería aplicar dicho Reglamento. Y por último, se fijan en ambos artículos cuales son los criterios determinantes y en qué medida la legislación europea es aplicable cuando el responsable o encargado del tratamiento no está establecido en la Unión Europea, siendo aquí una importante diferencia.²¹⁷

En aclaración, en lo relativo al sometimiento a la legislación Europa cuando el tratamiento de datos de carácter personal se produce por un establecimiento de la unión europea, las innovaciones de este nuevo reglamento son mínimas, en primer lugar, se añade que esto afecte no solo al responsable del tratamiento sino también al encargado de éste. En segundo lugar, que es independiente donde se realice el tratamiento, siempre que afecte a ciudadanos de la UE. Y por último, se elimina la mención a que el responsable este situado en varios Estados miembros puesto que el reglamento afecta a todos los Estados miembros. En este mismo sentido podemos observar el cambio del nuevo

²¹⁵ Vid. DE MIGUEL ASENSIO, P. A., *Aspectos internacionales del Reglamento General de protección de datos de la UE (II): Derecho aplicable*, (en línea). http://pedrodemiguelasensio.blogspot.com.es/2016/05/aspectos-internacionales-del-reglamento_19.html (consulta 16 de noviembre de 2016).

²¹⁶ *Ídem*.

²¹⁷ Artículo 3 RGPD.

considerando 22 el cual hace referencia clara a que un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables pero que no es un factor determinante la forma jurídica que resulte de él.²¹⁸ Pero sin duda los aspectos más controvertidos de modificación y posterior aplicación, en particular la proyección de la norma a entidades cuyo establecimiento responsable del tratamiento está afincado en un tercer Estado, ha perdido trascendencia en el nuevo Reglamento, ya que estas situaciones quedan comprendidas en el ámbito de aplicación del artículo 3.2 de éste.

Cabe destacar que conforme al criterio desarrollado por el TJUE en la sentencia Google Spain, que el tratamiento se produce en el marco de las actividades de un establecimiento cuando las actividades del responsable situado en un tercer Estado están indisociablemente ligadas a la de su establecimiento situado en el estado miembro de que se trate. Este vínculo puede existir aunque el establecimiento en la UE no participe en el tratamiento de datos. Esto con el nuevo artículo pierde parte de su importancia a consecuencia del nuevo enfoque de aplicación territorial introducido en él.²¹⁹ Aunque en su considerando 14 este reglamento establece que la protección en materia de datos personales debe aplicarse a toda persona física, independientemente de su nacionalidad, esto cambia cuando el responsable del tratamiento no se encuentra dentro de la UE, ya que la protección se limita a los interesados residentes de la Unión.²²⁰

En cuanto al criterio que dominaba anteriormente la Directiva 46/95 por el cual para que se aplicara la legislación europea, el responsable tenía que utilizar servidores ubicados en el territorio de la Unión los cuales utilizaba para recabar datos o incluso podía entenderse como tal los propios ordenadores de los individuos a través de las cookies o mecanismos similares, ahora bien, esto ha sido modificado por el mencionado artículo 3.2 ya que ha quedado bastante obsoleto con el avance fulgurante de las telecomunicaciones en especial Internet, ya que esta norma se remontaba a una época en la cual no estaba tan expandida. Esta nueva disposición refleja la evolución de la legislación en esta materia haciendo que el responsable que dirija su actividad en el marco del cual tiene lugar el tratamiento ya sea el Estado o la residencia del interesado pueda someterse a esta nueva legislación.²²¹ Se trata de un enfoque dado para facilitar el sometimiento a dicha legislación europea de quien no se encuentra dentro de la Unión en

²¹⁸ Considerando 22 del RGPD.

²¹⁹ DE MIGUEL ASENSIO, P. A., *loc cit.*

²²⁰ Considerando 14 del RGPD.

²²¹ DE MIGUEL ASENSIO, P. A., *loc cit.*

circunstancias donde interesa que queden bajo el control de este. De cara a la interpretación de este criterio nos podemos vasar en la jurisprudencia del TJUE relativa a que la actividad comercial vaya dirigida al Estado de la residencia habitual del consumidor, tal y como establece el Reglamento Roma I.²²²

Dado que las directrices del Reglamento Roma I son dadas para contratos de consumidores, hace falta extrapolarlas a este caso, ya que si bien no es un contrato de consumidores al uso, sí que en el caso concreto del tratamiento de datos y sobre todo de a quién va dirigida una actividad que se realiza a un particular, se puede utilizar este precepto, como ya bien lo estableció el TJUE en su jurisprudencia.²²³ Esta sentencia desautorizó las precisiones del considerando 24 del Reglamento Roma I, rechazando el criterio de la mera accesibilidad y estableciendo que *“la lengua o la divisa utilizada por un sitio de Internet no constituye un elemento pertinente para concretar el país al que la actividad va dirigida.”*²²⁴

La remarcada jurisprudencia del TJUE establece que para que se pueda determinar que un tratamiento va destinado a un particular en concreto y con eso a un Estado miembro en concreto, debe tener elementos que así lo establezca como pueden ser la mención de la dirección electrónica o portal del vendedor, la indicación de su número de teléfono o la utilización de una determinada lengua, tal y como establece el nuevo RGPD.²²⁵ El mismo reglamento, con carácter alternativo, establece que cuando el tratamiento de datos de interesados que residan en la unión esté relacionado con el control de su comportamiento siendo este en un lugar dentro de la Unión, también será de aplicación. Para esto, el Reglamento en su considerando señala que este criterio resulta operativo si se considera que una actividad que controla el comportamiento de los interesados, debe entenderse como parte de la actividad comercial propia de la empresa que trata dichos datos.²²⁶

En este nuevo bloque, se pueden observar varios cambios dentro de la normativa europea, uno de ellos es la incorporación de nuevos principios aplicables como pueden

²²² Artículo 6.1 del REGLAMENTO (CE) No 593/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (Roma I).

²²³ Sentencia del TJUE de 7 de diciembre de 2010. Asuntos acumulados. Caso *Peter Pammer* contra *Reederei Karl Schlüter GmbH & Co. KG* y *Hotel Alpenhof GesmbH* contra *Oliver Heller*

²²⁴ Considerando 24 Reglamento Roma I.

²²⁵ Considerando 23 RGPD.

²²⁶ Considerando 24 RGPD.

ser el principio de transparencia en el tratamiento de datos de carácter personal.²²⁷ Esto supone que el titular de estos datos tiene el derecho a estar informado de manera clara e inequívoca sobre el tratamiento que se está realizando, para que este pueda conocer en todo momento quién, cómo y para qué están siendo tratados sus datos personales, así como que datos concretamente son los que están siendo tratados. Con esto se debe reforzar la información que se les da a los titulares de los datos, tanto en el supuesto en que estos se recaben directamente del interesado como si se obtienen de otra fuente. El reconocimiento de este principio implica indirectamente, un aumento de la información que el responsable del fichero debe facilitar al titular de esos datos de carácter personal, siendo esto previo al momento en el que este obtenga los datos o cuando se aplique los ya obtenidos para otra finalidad.²²⁸ Por su parte el propio reglamento menciona expresamente el principio de responsabilidad²²⁹, que posteriormente desarrolla, que impone al responsable del fichero estar en condiciones de demostrar que cumple los principios aplicables de la protección de datos de carácter personal.²³⁰

Por otro lado, este Reglamento exige que el consentimiento a la hora de tratar los datos de carácter personal sea libre, informado, específico e inequívoco.²³¹ Para poder considerar este consentimiento de forma inequívoca, se necesita que los interesados acuerden dicho consentimiento a través de una acción positiva o una declaración, no puede deducirse dicho consentimiento del mero silencio o la omisión del interesado. Esta solicitud debe ser inteligible, de fácil acceso y con un lenguaje claro y sencillo.²³² El reglamento prevé que dicho consentimiento ha de ser explícito en algunos casos, como para cuando se utilicen datos sensibles, provocando así un reforzamiento de este consentimiento que no podrá ser dado de forma implícita con alguna que otra acción positiva, es necesario que una acción o declaración consintiendo explícitamente el tratamiento en cuestión.

Por último otro de los aspectos es que al igual que se ha dado el consentimiento se puede quitar, y es responsabilidad de los que traten dichos datos el demostrar que el

²²⁷ Artículo 5.1 a) RGPD.

²²⁸ MAYOR GÓMEZ R., “Contenido y novedades del reglamento general de protección de datos de la UE (reglamento UE 2016/679, de 27 de abril de 2016)”, en *Gabilex* nº 6 junio 2016

²²⁹ Artículo 5. 2 RGPD.

²³⁰ Artículo 24 RGPD.

²³¹ Artículo 4.11 RGPD. “«consentimiento del interesado»: 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”

²³² MAYOR GÓMEZ R., *loc cit.*

consentimiento se ha dado fehacientemente.²³³ Si hablamos de la edad en la que los menores pueden prestar por sí mismos su consentimiento para que se puedan tratar sus datos personales, el RGPD la establece en 16 años, todos los datos de menores de esa edad que se tengan que tratar, sería necesario el consentimiento de sus padres o tutores, esto hace una clara referencia a las redes sociales en las que cada vez, las gente crea sus perfiles con menos años. Esa edad puede ser rebajada por la legislación de cada Estado miembro siempre que no sea inferior a los 13 años, ya que se considera el límite mínimo. En España, el límite lo fija la AEPD y es de 14 años.²³⁴ Esto no afectará a las disposiciones generales del derecho contractual de los Estados, es decir que no por poder ceder los datos los niños de 14 años, significa que puedan celebrar contratos de consumo desde esa edad. En el caso de las empresas que recopilen los datos de menores, el consentimiento debe ser verificable, y el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan entender.²³⁵

Otro de los cambios de este nuevo reglamento son las nuevas categorías especiales de datos personales que se suman a las ya existentes (origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos, datos relativos a la salud o sexualidad e infracciones o condenas). A esta lista se añaden los datos genéticos y biométricos.²³⁶ El tratamiento de estos datos especiales pasa a estar prohibido siempre que se lleve a cabo con el fin de identificar de forma personal a un individuo.²³⁷ Ya en su capítulo tercero, el RGPD, describe los derechos que tienen los interesados, es decir los que son titulares de los datos tratados y que supone la introducción de nuevos derechos como el de supresión, el derecho al olvido y la portabilidad de datos y la superación de los derechos ARCO. La lista de derechos que tiene el titular de los datos es la siguiente: en primer lugar el derecho de transparencia (art 12), del cual hemos hablado ya en los

²³³ Artículo 7 RGPD.

²³⁴ Informe de la AEPD 2000-000: “En consecuencia, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales”.

²³⁵ Artículo 8 RGPD.

²³⁶ Artículo 4. 13 “datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona” y 4.14 “«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”

²³⁷ Artículo 9 RGPD.

principios de la norma, por otra parte están los derechos de información (arts. 13 y 14) y los ARCO (Acceso art 15; Rectificación art 16; Oposición art 21), si bien el derecho de cancelación que forma parte de los anteriores ha sido sustituido por el derecho de supresión o más comúnmente llamado derecho al olvido(art 17), combinándolo con el derecho a la limitación del tratamiento (art 18).

Uno de esos nuevos derecho es el derecho a la portabilidad de datos, que implica que el interesado que haya proporcionado sus datos a un responsable que los trate de modo automatizado puede solicitar la recuperación total o parcial de dichos datos en un formato que le permita su traslado a otro responsable. Cuando sea posible, el responsable deberá transferir los datos directamente al nuevo responsable designado por el interesado.²³⁸

Por otro lado, el cambio más importante de este nuevo Reglamento, es la introducción por primera vez en una norma del reconocimiento de un derecho al olvido digital, el cual solo había sido reconocido por la jurisprudencia anteriormente citada en este trabajo. Este derecho al olvido, tiene como objeto garantizar el derecho de los sujetos titulares de datos de carácter personal a obtener, sin dilación indebida, la supresión de los datos personales que le conciernan del responsable del tratamiento en determinados supuestos sobre todo, cuando los datos no sean necesarios para las finalidades para las que fueron recogidos. Por su parte, también serían motivo de eliminación estos datos, si estos datos hayan sido tratados ilícitamente o cuando la legislación así lo convenga.²³⁹

En cuanto al responsable de este tratamiento, el nuevo RGPD ha querido recalcar su responsabilidad para la aplicación de medidas técnicas y organizativas apropiadas, para garantizar el cumplimiento de esta norma. Se menciona la adhesión a códigos de conducta o un mecanismo de certificación digital.²⁴⁰ En este nuevo Reglamento, se elimina la obligación que existían antes de comunicar este a las autoridades de control y esto se sustituye por procedimientos y mecanismos eficaces que se centren en las operaciones que conlleven un alto riesgo para los derechos de los usuarios. Cada responsable o su

²³⁸ Artículo 20 RGPD

²³⁹ Todo el estudio de este derecho se ha visto en las anteriores partes de este mismo documento.

²⁴⁰ Artículo 24 RGPD.

representante tienen la obligación de llevar un registro de las actividades de este tratamiento, estando a disposición de las autoridades de control que lo soliciten.²⁴¹

Otra de las nuevas incorporaciones de este Reglamento es la obligación del responsable de avisar a las autoridades de control sin dilación indebida si se ha producido una violación de la seguridad de los datos personales, requiriéndose también la comunicación al interesado de dicha violación, esta comunicación ha de realizarse tan pronto como sea posible y en estrecha cooperación con la autoridad de control.²⁴² En este Reglamento se introduce la figura del delegado de Protección de Datos, que lo designara el responsable del tratamiento, se ente público o privado indistintamente. Sus actividades conllevarán la “observación habitual y sistemática de interesados a gran escala” y “el tratamiento a gran escala de categorías especiales de datos personales”.²⁴³ Este DPO puede ser un empleado de la plantilla de la empresa y podrá desempeñar otras funciones en las mismas siempre que no den lugar a conflictos de intereses. En cuanto a sus funciones, destacan el asesoramiento general dentro de la plantilla de lo relativo a la protección de datos, la supervisión del cumplimiento de la legislación y políticas de privacidad con especial atención a los riesgos asociados a las actividades que llevara a cabo la empresa, la elaboración de informes de evaluación de impacto de ciertos tratamientos de datos personales y la cooperación con las autoridades de control nacionales.²⁴⁴ Además en este reglamento, se hace hincapié en el traspaso de datos internacional, dando una especial protección a los datos que salen fuera de la unión europea, así como en la creación de un ente supranacional denominado Comité Europeo de Protección de Datos que será el que vele por el cumplimiento de las normas comunitarias en la materia, organismo que todavía no se ha creado en la actualidad.²⁴⁵

En resumen, se puede observar que en este nuevo Reglamento se introducen importantes novedades presentando aspectos muy relevantes como el hecho de implantar una regulación jurídica homogénea y uniforme para todos los Estados de la UE en este materia, lo que supone un beneficio tanto para los consumidores como para las propias empresas ya que consiguen seguridad jurídica y transparencia.²⁴⁶

²⁴¹ Artículo 30 RGPD.

²⁴² Artículo 33 RGPD.

²⁴³ Artículos de 37-39 del RGPD.

²⁴⁴ Mayor Gómez R., *loc cit.*

²⁴⁵ Artículos 44- 70 RGPD.

²⁴⁶ Mayor Gómez R., *loc cit.*

5. CONCLUSIONES

PRIMERA: Se debe entender que el derecho al olvido se crea como tal por una falta de seguridad de los datos que alberga internet, ya que estos no son susceptibles nunca de ser borrados. Dada la nueva era de comunicación que vivimos en nuestros días es lógico pensar que el derecho se tiene que modificar de tal manera que cubra las necesidades cada vez más importantes de este nuevo mundo llamado Internet, y una de esas necesidades es, sin duda, la protección de nuestros datos frente a terceros.

SEGUNDA: No podemos olvidar que este derecho surge de una evolución legislativa que se lleva a cabo en todos los países del mundo y que su esencia es extrapolada de varios preceptos ya vistos en nuestro ordenamiento, de tal forma que su implementación en nuestro ordenamiento jurídico no es tan drástica, ya que nos es en parte familiar.

TERCERA: Otra consideración primordial para entender el derecho al olvido es que su titular nunca dejará de serlo, haga lo que haga, o incluso si da permiso de acceso a estos datos al propio buscador. Esto es porque el derecho al olvido es un derecho que se puede ejercitar a lo largo del tiempo cuando se quiera, no caduca, ya que los datos previsiblemente objeto de este derecho quedan perennemente en internet y su acceso no está nunca limitado por el tiempo, así que no tendría sentido que se limitara el ejercicio de este derecho sobre unos datos que todavía pueden ocasionar perjuicios a su titular. Tal es la protección que en el caso de aceptar y ceder conscientemente estos datos a las empresas que se encargan de su tratamiento, el propio derecho da a su titular una facultad de romper ese acuerdo o sacar de él, los datos que le interese, otorgando así a una de las partes del acuerdo, un poder sobre la otra de control y de superioridad jurídica, que no existe en otros negocios jurídicos.

Bajo mi punto de vista, este poder que tiene el titular de los datos de poder “romper” esa cesión cuando considere oportuno no es sino otra de las demostraciones de la fuerza que desde las instituciones se le quiere otorgar al individuo frente a las grandes corporaciones que comercian con los datos personales como si se tratara de mercancía. Este derecho es una demostración del cambio de tendencia que se está llevando a cabo en todo el planeta, al considerar que los datos personales no pueden ser objeto de subasta entre empresas sin que su titular esté de acuerdo y mucho menos intentar amontonar

dichos datos personales sin establecer una diferenciación de aquellos que son susceptibles de herir sensibilidades y los que no.

CUARTA: Es completamente necesario tomar en consideración que este derecho al olvido tiene límites en su ejercicio y que por lo tanto no cualquier petición de supresión de datos debe atenderse, ya que no nos encontramos ante un derecho absoluto, sino que se modula y entra en conflicto con otros derechos intrínsecos a estos datos, como pueden ser el derecho a la libertad de expresión, a la publicidad y a la transparencia de la Administración, así como con los límites derivados de los fines históricos, científicos y de investigación.

QUINTA: Ya poniendo la vista en la sentencia principal que ocupa este trabajo, podemos extrapolar de ella que la legislación que regía en la UE en materia de protección de datos era una legislación bastante más laxa que los preceptos que se estaban llevando a cabo dentro de nuestro territorio, siendo nuestra legislación más rigurosa en este tema. Solo hay que observar que la sentencia del TJUE, que cambia completamente la manera de entender la protección de datos en Europa, confirma punto por punto las ideas principales de la AEPD plasmadas en su resolución. Creo que es una buena manera de ensalzar, en la medida de lo posible, a esta Agencia estatal, que vela por los intereses de los ciudadanos y que ha sido pionera en la lucha contra las grandes empresas y su forma de tratar los datos sensibles y personales.

SEXTA: Ahondando ya en la sentencia, debemos sacar en firme una idea muy clara y es que ésta, no discrimina entre datos veraces y datos que no lo son. Esta afirmación no es del todo exacta, puesto que siempre hay una protección especial contra los datos que no sean veraces, puesto que tienen la potestad de recurrir a la vía penal por injurias y calumnias, pero en el caso que nos corresponde, en el estricto margen de la protección de datos y al responsabilidad de los buscadores, no existe una diferencia notable. La sentencia condena moralmente a los buscadores de internet y los hace responsables de cualquier dato de carácter personal que tratan, indistintamente que este tratamiento sea en masa o sea individualizado, dando la potestad al individuo de ir en contra de este buscador si se quiere eliminar dicho rastro de internet. Esto puede no parecer del todo justo y ha habido muchas interpretaciones doctrinales sobre la

responsabilidad final del buscador y la impunidad que da esta sentencia a los sitios web donde están plasmados dichos datos.

La explicación que establece el TJUE sobre la limitación de esta responsabilidad solo a los buscadores, la basa en el derecho a la libertad de expresión y a la libertad de prensa que tiene los sitios web, principalmente periódicos y toda clase de blogs o páginas periodísticas, que no pueden ser limitados por este nuevo derecho al olvido, ya que estos derechos tienen una supremacía constitucional que este no tiene. Pero los buscadores y los motores que tratan los datos, no trabajan bajo la influencia de estos derechos de corte constitucional, por lo que pueden ser susceptibles de vigilancia y supresión desde la óptica del derecho al olvido.

Por todo ello, y según la nueva jurisprudencia establecida por el TJUE y de la mano con el nuevo Reglamento de protección de datos, se podrá exigir la retirada al buscador que indexa todo aquel dato que vulnere este derecho, pero esto no conlleva la retirada de las publicaciones comprometidas por parte de los sitios web.

SÉPTIMA: Ahora bien, no todos los datos indexados y tratados por un motor de búsqueda son susceptibles de eliminación, ni aun siendo datos considerados de carácter personal. Para que un particular interesado pueda exigir al motor de búsqueda la retirada de esos datos deberá acreditar que estos ya no son actuales, han perdido su interés público o son impertinentes e innecesarios, es decir, que estos datos no sean útiles para el público en general por estar desfasados ya sea por tiempo o por pérdida de interés. Es el propio buscador el que tiene la obligación de ejecutar, en primera instancia, un juicio paralelo sobre si mantener estos datos indexados o hacerlos desaparecer. El individuo pasa de ser un sujeto pasivo de los servicios de red a ser un sujeto activo.

Pero el problema radica en que es el propio individuo el que debe de solicitar dicha eliminación de los datos, quitando así la posibilidad de que sea el propio motor de búsqueda el que haga una criba de datos propensos a ser relacionados con el carácter personal del individuo. Se elimina la facultad que pudiera tener el buscador para actuar de oficio y poder modificar los resultados indexados, enrevesado muchísimo más el que para mi punto de vista es el espíritu de la sentencia, que no es otro que la protección de esos datos, independientemente de quien los quite, ya que se está obligando al usuario a

que tenga una visión global de todos sus datos dentro de la red para que pueda elegir cual le conviene y cual no, siendo una tarea casi imposible de realizar,

Sería lógico pensar que pueda ser el propio buscador el que hiciera un barrido provisional y eliminara los datos que pueda detectar que pudieran ser controvertidos y ahorrarnos la tarea de comprobar si mis datos han sido indexados, y tener que intentar eliminarlos por mi propia cuenta, en cambio tenemos un sistema que hace que los datos salgan a la luz sí o sí, y luego sea cada individuo el que se tenga que implicar para que estos desaparezcan cuando la mayoría del daño ya está hecho.

OCTAVA: En la argumentación seguida por el TJUE se plantea que sea el propio buscador el que una vez iniciado el trámite por el afectado, deba ponderar los intereses en juego, como son, en este caso, el derecho a la intimidad y a la propia imagen contra el derecho de expresión y de empresa. Darle este poder a un ente privado es una carga innecesaria, ya que no es del todo fiable que este ente que debe hacer a la vez de parte y de juez, tenga una actuación equitativa y justa para con los individuos interesados.

Esta acción debería ser una ponderación extrajudicial de la actuación del propio buscador, pero queda en manos de una empresa cuya finalidad es la recopilación de datos y su indexación. Resulta raro que se le adjudique a este ente privado una potestad arbitral cuando lo que hay en juego son derechos fundamentales que pueden llegar a afectar a muchísimas personas.

NOVENA: Para terminar, hemos de reflexionar sobre el futuro jurídico en lo que se refiere a Internet. El nuevo reglamento Europeo ha supuesto un gran avance respecto a las políticas nacionales de cada miembro europeo, siendo España uno de los países que menos va a tener que cambiar su política con respecto a este último ya que es una de las políticas más avanzadas de la zona.

La regulación de internet es un desafío constante para los juristas. Nos enfrentamos ante una realidad novedosa y cambiante y la ley debe cambiarse y modificarse a un ritmo acelerado para poder dar soluciones justas a los conflictos que se producen en esta sociedad tecnológica en la que vivimos, pero sin olvidar que el objetivo primordial es la defensa de los derechos y los intereses de las personas.

6. BIBLIOGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Declaración sobre buscadores de Internet”, *RAEPD*, 1 de diciembre de 2007.
- ÁLVAREZ RIGAUDIAS, C. “Sentencia Google Spain y Derecho al Olvido” en *Actualidad Jurídica Uría Menéndez* 2015
- ARENAS RAMIRO, M. “Hacia un futuro derecho al olvido de ámbito europeo”, *La protección de los datos personales en internet ante la innovación tecnológica*, Aranzadi, Cizur Menor, 2013.
- CASINO RUBIO, M. “El periódico de ayer, el derecho al olvido en Internet y otras noticias”, *Revista española de Derecho Administrativo*, Civitas, n.º. 156/2012
- CHANAMÉ ORBE, R., *Habeas Data y el Derecho Fundamental a la Intimidad de la Persona*. Tesis Doctoral (s.p.), Universidad Nacional Mayor de San Marcos, Lima, 2003.
- CÓRDOBA CASTROVERDE, D. “El derecho al olvido tras la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014”, en *ELDERECHO.COM*
- DE MIGUEL ASENSIO, P. A., *Aspectos internacionales del Reglamento General de protección de datos de la UE (II): Derecho aplicable*, (en línea).
- DIEZ-PICAZO, L. y GULLÓN, A. *Sistema de Derecho Civil*, Vol. II, Tecnos, 9ª ed., Madrid, 2003.
- GARRIGA DOMÍNGUEZ, A. *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2009.
- GOMES ANDRADE. N.N. “El olvido: el derecho a ser diferente de uno mismo. Una reconsideración del derecho a ser olvidado”, *IDP*, núm. 13, febrero 2012.
- GUICHOT, E., “La publicidad de datos personales en Internet por parte de las Administraciones públicas y el derecho al olvido”, *REDA*, núm. 154, 2012
- MARTINEZ OTERO, J.M. “El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja”, *UNED. Revista de Derecho Político*, n.º 93, mayo-agosto 2015
- DE MIGUEL ASENSIO, P. A., *Aspectos internacionales del Reglamento General de protección de datos de la UE (II): Derecho aplicable*, (en línea).
- MILL, J.S. *On Liberty. En Prefaces to Liberty*. Bacon Press. Boston 1959.

- NOVAL LAMAS, J.J. “Derecho al olvido: algunas consideraciones sobre su futura regulación”, *RCE*, N°: 120, Octubre-Diciembre 2012.
- NOVOA, E. “El Derecho a la Vida y Libertad de Expresión”. *Editorial Siglo XXI*. México. Cuarta Edición. México. 1989
- OST, F. “El tiempo del derecho” *Siglo XXI editores*, México, 2005.
- PALACIOS GONZÁLEZ, M. D., “El poder de autodeterminación de los datos personales en internet”, *IDP*, número 14, mayo 2012
- PEREZ LUÑO, A. *Derechos Humanos, Estado y Constitución*. Editoriales Tecnos. Madrid.
- SIMÓN CASTELLANO, P. “El derecho al olvido en internet” en *La libertad de expresión e información en internet*.
- SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE*, Bosch, Barcelona 2015.
- TERWANGNE, C. “Privacidad en Internet y el derecho a ser olvidado/derecho al olvido”. *IDP: Revista de Internet, derecho y política*, n°13, 2012
- TRUDEL, P. “*Lóubli en tant que droit et obligation dans les systèmes juridiques civilistes*”
- UGARTE CATALDO, J.L. “El derecho a la intimidad y la relación laboral” en *Boletín oficial dirección del trabajo*, n° 139/2000
- VÁZQUEZ DE CASTRO, E., “Protección de datos personales, redes sociales y menores”, *Revista Aranzadi de Derecho y Nuevas Tecnologías (RDNT)*, n°. 29, mayo-agosto 2012.