UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja

Derecho a la Privacidad y Nuevas Tecnologías: jurisprudencia del TJUE.

Trabajo fin de máster presentado por:	Lidia Sigüeiro Couselo
Titulación:	Máster en Propiedad Intelectual y Derecho de las Nuevas Tecnologías
Línea de investigación:	Cuestiones jurídicas respecto la privacidad y protección de datos, tanto en los modelos europeos como anglosajones.
Director/a:	Dña. Cristina Paredes Serrano

A Coruña
10 de diciembre de 2015
Firmado por: Lidia Sigüeiro Couselo

CATEGORÍA TESAURO: (3.15.) Derecho Privado

ÍNDICE:

Págs.

I. RESUMEN 5
II. INTRODUCCIÓN 6
III. DESARROLLO 8
III.1. ARTÍCULO 18.4 DE LA CONSTITUCIÓN ESPAÑOLA 8
III.1.1. Derecho a la Intimidad y artículo 18 de la Constitución Española.. ... 29
III.1.2. Creación jurisprudencial del Derecho a la Protección de Datos de Carácter Personal. 10
III.1.3. Derecho a la Privacidad..... 14
III.2. TRANSFERENCIAS INTERNACIONALES DE DATOS Y SAFE HARBOR..... 17
III.2.1. Transferencias internacionales de datos a países situados fuera de la Unión Europea. 18
III.2.2. Principios de puerto seguro (Safe Harbor) y Decisión 2000/520/CE de la Comisión de 26 de julio de 2000. 23
III.2.3. Estados Unidos y la Privacidad. Caso Snowden. 26
III.2.4. Sentencia del TJUE de 6 de octubre de 2015. 27
III.2.5. Futuro de las transmisiones internacionales de datos a Estados Unidos..... 32
III.3. DERECHO AL OLVIDO..... 35
III.3.1. Derecho al olvido y su relación con los artículos 10.1 y 18.4 de la Constitución Española..... 37
III.3.2. Reconocimiento del derecho al olvido por la AEPD y las Agencias de Protección de Datos Europeas..... 40
III.3.3. Sentencia del TJUE de 13 de mayo de 2014 y conclusiones del abogado general. 41
III.3.4. Consecuencias de la Sentencia del TJUE de 13 de mayo de 2014. . 48
III.3.5. Sentencia del TS. 53
III.3.6. Inclusión del derecho al olvido en la Reforma de la Directiva 95/46/CE.. 55
III.3.7. Derecho al olvido en el common law. 56
III.4. CONSERVACIÓN DE DATOS 57
III.4.1. Directiva 2006/24/CE y Ley 25/2007, de 18 de octubre, de conservación de datos..... 58
III.4.2. STJUE de 8 de abril de 2014..... 60
III.4.3. Consecuencias STJUE de 18 de abril de 2014 y de la reforma de la LCrim..... 62
IV. CONCLUSIONES..... 65
V. FUENTES JURÍDICAS UTILIZADAS..... 69

Abreviaturas:

- AEPD: Agencia Española de Protección de Datos.
- CE: Constitución Española.
- EEUU: Estados Unidos.
- LOPD: Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- NSA: National Security Agency.
- SAN: Sentencia de la Audiencia Nacional.
- STC: Sentencia del Tribunal Constitucional
- STJUE: Sentencia del Tribunal de Justicia de la Unión Europa.
- STS: Sentencia del Tribunal Supremo.
- TC: Tribunal Constitucional.
- TJUE: Tribunal de Justicia de la Unión Europea.
- TS: Tribunal Supremo.

AGRADECIMIENTOS:

A mi familia por haber hecho posible la existencia de este trabajo y por haberme apoyado siempre.

A todos y cada uno de los profesores del Máster en Propiedad Intelectual y Nuevas Tecnologías de la UNIR.

I. RESUMEN

Derecho a la Privacidad y Nuevas Tecnologías: jurisprudencia del TJUE.

Las nuevas tecnologías suponen un reto para la preservación del derecho a la privacidad de las personas. Cuando hablamos de derecho a la privacidad debemos distinguir éste del derecho a la intimidad y comprender que abarca una esfera mucho más amplia. El Tribunal de Justicia de la Unión Europea, en los últimos años, ha dictado diversas Sentencias que resultan de especial relevancia para definir los límites del derecho a la privacidad. Entre las Sentencias más destacadas nos encontramos la que reconoció y fijo los límites del derecho al olvido; la que invalidó la Directiva europea de conservación de datos y la reciente Sentencia de 6 de octubre, que invalidó la Decisión en la que se amparaba la legalidad de los acuerdos de Safe Harbor con Estados Unidos. Todas estas Sentencias ponen de manifiesto las diferencias existentes entre la interpretación del derecho a la privacidad en los modelos jurídicos europeos y anglosajones.

Palabras Clave: “Privacidad”, “Safe Harbor”, “Derecho al Olvido”, “Conservación de Datos”, “Protección de Datos”

Abstract

Privacy Law and New Technologies: ECJ case law.

New technologies constitute a challenge to the preservation of the right to privacy. When we talk about the right to privacy we must distinguish between privacy and intimacy, and understand that the first covers a much broader scope. In the last few years, the Court of Justice of the European Union has issued several judgments that are particularly important to define the limits of the right to privacy. Among the most important cases we can highlight the following: a case that has recognized and fixed the limits of the right to be forgotten; a second judgment that has invalidated the European Data Retention Directive; and the most recent, from October 6th, that has questioned the legality of the Safe Harbor agreements with the United States. All these cases illustrate the differences between the interpretation of the right to privacy in European and Anglo-Saxon legal models.

Keywords: "Privacy", "Safe Harbor", "Right to be Forgotten”, "Data Retention", "Data Protection"

II. INTRODUCCIÓN

La irrupción de las nuevas tecnologías en la sociedad ha supuesto un gran reto para nuestro ordenamiento jurídico, que desde el origen de las mismas se ha visto incapaz de actualizarse con la misma rapidez que los avances tecnológicos lo han requerido.

Nos encontramos ante un nuevo escenario social que, si bien implica entre otras cosas un gran avance para la sociedad, puede poner en riesgo derechos personales fundamentales.

Entre los derechos afectados por las nuevas tecnologías nos encontramos con el derecho a la privacidad, cómo el más susceptible de ser vulnerado debido al mal uso de las mismas. La esfera personal del individuo puede quedar al descubierto fácilmente a través de internet, o de alguno de los medios electrónicos que usamos para comunicarnos.

El derecho a la privacidad de las personas surgió en Europa como un derecho autónomo, estrechamente relacionado con el derecho a la intimidad, pero distinto a éste y con un contenido más amplio.

Mientras que en los países pertenecientes a la Unión Europea el derecho a la privacidad se reconoce como un derecho fundamental, en Estados Unidos éste parte de una creación jurisprudencial. Esta diferencia es la que provoca la distinta forma de ver la privacidad en ambos sistemas jurídicos.

En los últimos años el Tribunal de Justicia de la Unión Europea se ha pronunciado a través de diversas Sentencias a favor de un aumento de la protección del derecho a la privacidad, definiendo el alcance de las garantías del mismo.

Se examinará la reciente anulación de los acuerdos del Safe Harbor o puerto seguro por el Tribunal de Justicia de la Unión Europea el pasado 6 de octubre de 2015. Con dicha Sentencia ha quedado patente más que nunca la tensión provocada por las diferentes formas de ver la privacidad en Europa y en Estados Unidos.

Otro de los puntos a tratar en el presente trabajo será el famoso “Derecho al Olvido”, consolidado por la Sentencia del TJUE de 13 de mayo de 2014. En el caso del

"Derecho al Olvido", la mayor controversia se encuentra en dar prioridad a éste o al derecho a la libertad de expresión.

Finalmente, cabe también plantearse como afecta al derecho a la privacidad, el hecho de que las operadoras de telecomunicaciones se encuentren obligadas a conservar determinados datos de nuestras comunicaciones personales.

El TJUE ha dictado una Sentencia a través de la cual declaró inválida la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, por su injerencia en derechos fundamentales de la persona.

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, no deja de ser la transposición de la directiva invalidada y actualmente se sigue aplicando en España a pesar de lo dispuesto en la Sentencia del TJUE.

La finalidad del presente trabajo es investigar las garantías que la reciente jurisprudencia del TJUE ha fijado en relación con el derecho a la privacidad. Para ello, se intentará definir primero lo que es el derecho a la privacidad y como en nuestro país se encuentra protegido como un derecho fundamental a través del artículo 18.4 de la Constitución Española.

III. DESARROLLO

III.1. ARTÍCULO 18.4 DE LA CONSTITUCIÓN ESPAÑOLA

Siendo el título del presente trabajo "*Derecho a la Privacidad y Nuevas Tecnologías*", no podemos dejar de tomar como referencia para el desarrollo del mismo el apartado 4 del artículo 18 de la Constitución Española, el cual fue introducido en la misma por el legislador en el año 1978, sin poder éste ni imaginarse en ese momento la repercusión que internet acabaría teniendo en nuestras vidas.

III.1.1. Derecho a la Intimidad y artículo 18 de la Constitución Española.

El artículo 18 de la Constitución en un inicio lo que pretendía regular era el llamado Derecho a la Intimidad, cuyo origen se encuentra en el artículo 12 de la Declaración Universal de Derechos Humanos de 1948:

"12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". [1]

Así mismo, dos años más tarde, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales dispuso en relación con el Derecho a la Intimidad lo siguiente:

"8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
8.2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho salvo cuando esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros". [2]

El Derecho a la Intimidad puede definirse por lo tanto, siguiendo la definición aportada por Víctor Salgado, de la siguiente forma:

[1] Artículo 12. Declaración Universal de los Derechos Humanos. 10 de diciembre de 1948.
[2] Artículo 8. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. 4 de noviembre de 1950.

"A efectos prácticos, podemos definir la intimidad como una esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas o conocimiento de terceros, salvo excepciones muy concretas contenidas en la Ley. Dicha esfera protege tanto elementos físicos e instrumentales (como la propia vivienda, la correspondencia o las comunicaciones privadas), como elementos sustanciales que suponen determinados datos sensibles sobre el individuo (su ideología, religión, creencias, vida sexual o salud).

La intimidad es, pues, un derecho fundamental clásico en nuestro acerbo jurídico y ha sido objeto de un amplio desarrollo tanto legislativo como jurisprudencial en nuestro país".[3]

Pues bien, teniendo en cuenta la tendencia recogida en la Declaración Universal de los Derechos Humanos y en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, y como ya se ha mencionado previamente, en el año 1978 el legislador quiso dotar a la Constitución de un artículo que regulase el Derecho a la Intimidad.

Sin embargo, a mayores de las previsiones que incluían el derecho al honor, a la inviolabilidad del domicilio y al secreto de las comunicaciones (todos ellos previstos en la Declaración Universal de los Derechos Humanos de 1948), el legislador fue más allá e introdujo una limitación al uso de la informática, que se materializó en el apartado 4 del Artículo 18 de la Constitución:

"Artículo 18
Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
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". [4]

Cabe recordar que en el año 1978, poco podía imaginarse el legislador sobre el papel que las nuevas tecnologías iban a tener en nuestras vidas, por lo que la interpretación sobre el alcance del apartado 4 de este artículo 18 de la Constitución

[3] SALGADO SEGUÍN (2010 : 69-79).
[4] Artículo 18. Constitución Española. 29 de diciembre de 1978.

ha sido objeto de controversia a lo largo de los años, hasta derivar en lo que hoy conocemos en el derecho a la protección de datos de carácter personal o derecho a la autodeterminación informativa.

III.1.2. Creación jurisprudencial del Derecho a la Protección de Datos de Carácter Personal.

Como se ha reflejado en el apartado anterior, la inclusión por parte del legislador de una limitación al uso de la informática a través del apartado 4 del artículo 18 de la Constitución, ha supuesto un problema a la hora de interpretar el alcance de dicha limitación.

Han sido los tribunales, especialmente el Tribunal Constitucional, los que han dotado de sentido a este artículo a través de diferentes Sentencias, entre las que podemos destacar la STC 254/1993, de 20 de julio de 1993 y la STC 292/2000, de 30 de noviembre de 2000.

Una de las primeras interpretaciones realizadas por el Tribunal Constitucional en relación con el artículo 18 de la Constitución, ha sido la realizada en su Sentencia STC 110/84, de 26 de noviembre de 1984, en la que ponía de manifiesto que los distintos apartados del artículo 18 de la Constitución:

"(...) tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de la tecnología, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esta protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad, y del respeto a la correspondencia que es o puede ser medio de conocimiento de aspectos de vida privada".[5]

Como se puede observar, la STC 110/84 supone un primer avance hacía lo que hoy conocemos como del derecho a la protección de datos de carácter personal, al reconocer el TC que la inclusión del apartado 4 del artículo 18 de la Constitución tiene su razón de ser en excluir el ámbito de la vida privada, personal y familiar del conocimiento ajeno a través de las intromisiones de la tecnología.

[5] STC 110/84 de 26 de noviembre de 1984.

Sería con la STC 254/1993, de 20 de julio de 1993, con la que se comenzaría a hablar de un "derecho a la libertad informática", en palabras del TC:

"Dispone el art. 18.4 C.E. que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que 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»"[6].

Analizando el contenido de la STC 254/1993, y siguiendo la doctrina de Antoni Roig, podemos observar que se trata el "derecho a la libertad informática" como una vertiente positiva del derecho a la intimidad. Con esta Sentencia el TC no define todavía por completo el alcance de la limitación prevista en el apartado 4 del artículo 18:

"En la STC 254/1993, de 20 de julio, se describe un derecho de contornos todavía imprecisos, llamado "libertad informática". Esta decisión es ecléctica. En efecto, se afirma en primer lugar la existencia de un "derecho a la libertad informática" como derecho o libertad autónomo. Ahora bien, este derecho se vincula, en segundo lugar, al derecho a la intimidad, pues no es sino su vertiente positiva.

Así, si el ciudadano puede negar la difusión de ciertos datos (vertiente negativa), debería poder asimismo disponer de facultades positivas para oponerse a su conservación, una vez desaparecida la finalidad que llevó a su obtención, o a su cesión a terceros sin mediar autorización"[7].

La relación establecida por la STC 254/1993 entre el derecho a la intimidad y la denominada libertad informática, dejaba fuera de juego la protección de determinados datos personales de los individuos que no pertenecían estrictamente al ámbito de la intimidad.

No sólo los datos que afectan a la intimidad de las personas son los que se deben incluir en la protección otorgada por el artículo 18.4 de la Constitución, puesto que a

[6] STC 254/1993 de 20 de julio de 1993.
[7] ROIG BATALLA (2011 : 14).

través de las nuevas tecnologías se pueden conocer otro tipo de datos que pueden resultar peligrosos para las personas, o hacerlas identificables, configurando un determinado perfil de las mismas que puede ser ideológico, sexual, religioso o de cualquier otra índole.

La solución al problema de la protección de datos de carácter personal que no estaban protegidos por el derecho a la intimidad, vino dada por el TC en su Sentencia STC 292/2000, de 30 de noviembre de 2000.

El TC a través de la STC 292/2000, reconoció la singularidad y autonomía del derecho personal a la protección de datos, y comenzó a tratar a éste como un derecho independiente del derecho a la intimidad, mediante el cual se reconoce el derecho de las personas a disponer y controlar sus datos personales frente a terceros que puedan acceder a ellos sin su autorización. En palabras del TC:

" (...) La función del derecho fundamental a la intimidad del art. 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 (por todas STC 144/1999, de 22 de julio, FJ 8). 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 derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información.

Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin. De ahí la singularidad del derecho a la protección de datos, pues, 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 sólo 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 octubre, 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.

El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo (...)".[8]

La STC 292/2000, resulta por lo tanto fundamental en la interpretación del apartado 4 del artículo 18 de la Constitución, definiendo su alcance y dando solución al problema de qué datos deben protegerse en virtud del mismo.

Nos encontramos ante un nuevo derecho, que permite al ciudadano decidir cuáles de sus datos se van a tratar y con qué finalidades, y que le otorga los derechos de acceso, rectificación, cancelación y oposición sobre los mismos (conocidos como derechos ARCO).

Antoni Roig, señala en relación a lo que se debe considerar por datos personales y a la función del derecho a la protección de los mismos lo siguiente:

"La función es distinta, en primer lugar, puesto que el derecho a la intimidad protege frente a invasiones en la esfera personal y familiar. En cambio, el derecho a la protección de datos personales garantiza al ciudadano un poder de control o de disposición sobre el uso y el destino de sus datos personales. En segundo lugar, también el objeto de ambos derechos difiere. Los datos personales no son

[8] STC 292/2000 de 30 de noviembre de 2000.

únicamente los datos íntimos de la persona, sino que incluyen, de manera más amplia, todos aquellos que identifiquen o permitan la identificación de la persona".[9]

La STC 292/2000, no hace sino confirmar una realidad existente en España en el momento de publicación de la misma. Distintas voces como la del magistrado Pablo Lucas Murillo de la Cueva, ya abogaban por la creación de un nuevo derecho fundamental consistente en la protección de datos de carácter personal.

En 1992, la exposición de motivos de Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, ya defendía la diferencia entre en concepto de intimidad y el concepto de privacidad.

En palabras del magistrado Pablo Lucas Murillo de la Cueva:

"no hay que olvidar que el derecho a la autodeterminación informativa es un derecho fundamental. Que se dirige a satisfacer una necesidad básica de toda persona: el control de la información que le concierne. Que no consiste en una exquisitez jurídica ni en un capricho, sino en una pretensión esencial en la sociedad en que vivimos. Sin ese control, sin los límites que comporta para los poderes públicos y para los sujetos privados, ya sean los gobernantes, ya sean las empresas u otras entidades privadas, contarán no sólo con un conocimiento potencialmente pleno de la vida de cada uno de nosotros, sino que lo utilizarán para tomar decisiones que nos afectarán directa o indirectamente pero siempre de manera decisiva. El resultado será que estará en peligro el libre desenvolvimiento de nuestra vida e, incluso nuestra propia identidad."[10]

III.1.3. Derecho a la Privacidad.

Debemos distinguir entre el Derecho a la Intimidad y el Derecho a la Privacidad. Hasta la Sentencia del Tribunal Constitucional 292/2000, se interpretaba el artículo 18.4 como la *vertiente "positiva" del Derecho a la Intimidad*[11], mientras que a partir de la publicación de dicha Sentencia, el mencionado artículo se relaciona indudablemente con el Derecho a la Protección de Datos.

Sin embargo, no todos los derechos afectados por la irrupción de las nuevas tecnologías quedan comprendidos en el derecho a la protección de datos, motivo por

[9] ROIG BATALLA (2011 : 15).
[10] MURILLO DE LA CUEVA. (2007: 30).
[11] ROIG BATALLA (2011 : 14).

el cual es necesario seguir un concepto amplio de derecho a la privacidad en el análisis del presente trabajo.

El derecho a la privacidad, ya había sido definido en España con carácter previo a la STC 292/2000, en 1992 en la exposición de motivos de Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal se afirmaba lo siguiente:

"El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".[12]

Según Víctor Salgado, una definición del Derecho a la Privacidad podría ser la siguiente:

" (...) La Privacidad sería así una nueva esfera, mucho más amplia que la de la propia intimidad, que contendría ni más ni menos que todos los datos vinculados a un individuo, sean éstos sensibles o no, los cuales deben ser controlados y protegidos en su tenencia y tratamiento por parte de terceros. [13]

En Europa, el derecho a la privacidad se ha protegido normativamente mediante el Convenio 108 del Consejo de Europa de 1981, por la Directiva Europea 95/ 46/CE de 1995 y por el artículo 8 de la Carta Europea de Derechos Fundamentales, que recoge lo siguiente:

«Protección de datos de carácter personal:

12 Exposición de motivos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

[13] SALGADO SEGUÍN. (2010 : 69-79)

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

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

Sin embargo, en el sistema jurídico anglosajón el concepto de Derecho a la Privacidad surgió en un artículo jurídico de 1890 (Brandeis & Warren), en el cual se definió como "*the right to be let alone".* La base de dicho artículo consistía en impedir que el Estado pueda interferir en la vida de las personas sin su autorización o sin una autorización judicial fundamentada. Según Víctor Salgado:

" (...) c*on base en el citado artículo y siguiendo el peculiar sistema de creación de derecho anglosajón, basado tanto en el precedente judicial como en la propia ley, se fue reconociendo el citado derecho en el sistema norteamericano, incorporando principios como la inviolabilidad del domicilio, la correspondencia o, más recientemente, las telecomunicaciones".*[14]

"Sin embargo, esta 'estandarización internacional' se encuentra con una dificultad trascendental: la fuerte colisión entre dos modelos normativos contrapuestos: el modelo europeo y el modelo americano. Dicho choque evidencia la concepción tan distinta que europeos y americanos tenemos sobre la 'privacidad'. Para un estadounidense, el derecho a la privacidad no es un derecho fundamental reconocido por su Constitución, a diferencia de, por ejemplo, la libertad de expresión recogida en su famosa 'Primera Enmienda'. Dicho derecho, por tanto y tal y como hemos visto, fue creado y perfilado por la propia jurisprudencia americana suponiendo, en la práctica, una protección muy parecida a nuestro derecho a la intimidad (es decir, inviolabilidad del domicilio, secreto de las comunicaciones y protección de la vida privada).

Por el contrario, visto lo analizado, para un europeo la privacidad es algo muy distinto. Dado que nuestra legislación reconoce y protege ya todos estos aspectos mediante el derecho a la intimidad, la privacidad ha surgido como una esfera de protección más amplia. Dicha esfera abarca todos los datos que cualquier entidad tenga sobre un ciudadano, y no solamente los estrictamente privados. En Europa,

[14] SALGADO SEGUÍN. (2010 : 69-79).

por tanto, el derecho a la privacidad no es otra cosa que el derecho que protege a las personas físicas en relación al tratamiento de sus datos por parte de terceros o, dicho de otro modo, el derecho a la protección de datos de carácter personal.

También, a diferencia de EEUU y como hemos visto, en Europa el derecho a la privacidad se protege como un derecho fundamental, recogido tanto en el artículo 18.4 de nuestra Constitución como en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, además de ser desarrollado por la LOPD y por la Directiva Europea 95/46/CE.

Estas diferencias son muy notables y, habida cuenta de que EEUU ha sido la cuna de Internet y es donde se ubican las principales empresas proveedoras de sus servicios a nivel mundial, como Google, Facebook, Microsoft o Apple (cuyos modelos de negocio se copian también en Europa), se están creando importantes problemas jurídicos con una gran trascendencia práctica (...)"[15].

La diferencia entre ambos modelos jurídicos (el anglosajón y el europeo) es la base de muchos de los conflictos que existen en la actualidad en relación con el derecho a la privacidad y que se analizará a lo largo del presente trabajo.

III.2. TRANSFERENCIAS INTERNACIONALES DE DATOS Y SAFE HARBOR

Como ha quedado patente en el apartado anterior, las diferencias entre la forma de ver la privacidad entre Europa y Estados Unidos, suponen la aparición de problemas jurídicos con una gran transcendencia práctica.

Mientras que para Europa la privacidad es un derecho fundamental y el derecho a la protección de datos se encuentra plenamente regulado por la Directiva Europea 95/ 46/CE de 1995, para Estados Unidos la privacidad no es un derecho fundamental, si no un derecho de creación jurisprudencial.

Uno de los principales problemas que supone la diferencia a la hora de interpretar el concepto de privacidad entre Europa y Estados Unidos, nos lo encontramos al constatar que las transferencias internacionales de datos entre ambos territorios son masivas. Los datos principalmente se transfieren desde la Unión Europea a Estados

[15] SALGADO SEGUÍN (2010 : 69-79).

Unidos, con el consiguiente problema del recelo de los legisladores de la Unión ante la menor importancia que se le concede a la privacidad en Estados Unidos.

Hasta el 6 de octubre de 2015, dichas transferencias estaban amparadas por la decisión 2000/520/CE de la Comisión Europea, que reconocía que los acuerdos de Safe Harbor o puerto seguro otorgaban una protección equivalente en el tratamiento de los datos a la que garantiza la directiva 95/46/CE.

Sin embargo, el pasado 6 de octubre de 2015, a raíz una denuncia presentada por un ciudadano austriaco, el Sr. Schrems, ante la autoridad irlandesa de control, considerando que, las revelaciones realizadas en 2013 por el Sr. Edward Snowden en relación con las actividades de los servicios de información de Estados Unidos (en particular, la National Security Agency o «NSA»), no garantizaban una protección suficiente de los datos transferidos a ese país, el Tribunal de Justicia de la Unión Europea dictó una Sentencia que ha invalidado la decisión 2000/520/CE.

La anulación de los acuerdos de Safe Harbor supone un escenario incierto en la actualidad, en el que las empresas a la espera de que se negocie un nuevo Safe Harbor que sí cumpla con los requisitos necesarios para otorgar a los datos transferidos una protección equivalente a la de la Unión Europea, tienen hasta el 29 de enero de 2016 para adaptarse a la nueva situación.

III.2.1. Transferencias internacionales de datos a países situados fuera de la Unión Europea.

Para comprender mejor el conflicto que ha supuesto la anulación de los acuerdos de Safe Harbor, debemos analizar primero el régimen europeo de transferencias internacionales de datos y lo que dice la normativa española al respecto.

En la Unión Europea, las transferencias internacionales de datos se encuentran reguladas principalmente a través de los artículos 25 y 26 de la Directiva 95/46/CE:

“Artículo 25

Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de

datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

(...)

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión"[16].

Como se puede observar, la base para la realización de transferencias internacionales de datos a terceros países desde la Unión Europea, es que éstos garanticen un nivel de protección adecuado para dichos datos.

En España, las disposiciones acerca de la transmisión internacional de datos se regulan en los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el Título VI 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.

Según la normativa española, y atendiendo a lo dispuesto en el artículo 5 de la LOPD[17], se considera que un tratamiento de datos que suponga la transmisión de los mismos fuera del territorio del Espacio Económico Europeo será considerado siempre una transferencia internacional de los mismos. Es indiferente que dicho tratamiento tenga por objeto la cesión o la comunicación de los datos, o la realización de un tratamiento de los datos por cuenta del responsable del fichero establecido en territorio español.

[16] Artículo 25. Directiva 95/46/ce del parlamento europeo y del consejo de 24 de octubre de 1995
[17] Artículo 5 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Nos encontramos ante dos figuras, la del exportador de los datos (persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero) y la del importador de los datos (la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, ya sea responsable del tratamiento, encargado del tratamiento o tercero).

La normal general sobre las transferencias internacionales de datos se encuentra recogida en el artículo 33 de la LOPD:

"Artículo 33 Norma general

1. *No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.*

2. *El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*[18]

Como podemos deducir de la lectura del artículo 33, están prohibidas las transferencias internacionales de datos a países que no proporcionen un nivel de protección equiparable al de la LOPD española, salvo autorización del Director de la Agencia de Protección de Datos y observación de las garantías adecuadas para la protección de dichos datos.

Esta regla general viene acompañada de una serie de excepciones recogidas en el artículo 34 de la LOPD y reguladas en el Real Decreto 1720/2007, de 21 de diciembre.

Algunas de las excepciones más reseñables son las siguientes:

[18] Artículo 33 LOPD.

Artículo 34 Excepciones

Lo dispuesto en el artículo anterior no será de aplicación:

> *(...)* ***e)*** *Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.*
>
> ***f)*** *Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.*
>
> ***g)*** *Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero. (...)*
>
> ***k)*** *Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.*[19]

En el caso que nos ocupa, la anulación de las reglas de Safe Harbor tiene especial relevancia el apartado k) del artículo 34, con respecto a transferencias internacionales de datos a países en los que la Comisión Europea garantiza un nivel de protección adecuado para los mismos.

Se hace también incidencia en esta excepción en el artículo 68 del Real Decreto 1720/2007, de 21 de diciembre:

"Artículo 68

Nivel adecuado de protección declarado por Decisión de la Comisión Europea

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección"[20]*.*

A pesar de que los acuerdos de Safe Harbor se han anulado por la STJUE de 6 de octubre de 2015, sigue habiendo países que están considerados por la Comisión Europea como seguros para la realización de transferencias internacionales de datos.

[19] Artículo 34 LOPD.
[20] Artículo 68 Reglamento LOPD.

Un listado actualizado de estos países (y de las decisiones por las cuales se les considera seguros para las transferencias internacionales de datos a los mismos) lo podemos encontrar en la página web de la Agencia Española de Protección de Datos[21]:

- Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000
- Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos
- Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003
- Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
- Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
- Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
- Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
- Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
- Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
- Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012
- Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012

Finalmente, no podemos dejar de tener en cuenta que la transmisión de datos internacionales a países que no proporcionen un nivel de protección equiparable al de la LOPD, sin la autorización del Director de la AEPD, consiste en una infracción muy grave recogida en el artículo 44.4, apartado d) de la LOPD:

"44.4. Son infracciones muy graves:

(...) d)

La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que

[21] AEPD. Consultado en : https://www.AEPD.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria".[22]

La comisión de infracciones muy graves está penada por la LOPD con una sanción consistente en una multa que puede oscilar entre los 301.000 € y los 600.000 €.[23]

III.2.2. Principios de puerto seguro (Safe Harbor) y Decisión 2000/520/CE de la Comisión de 26 de julio de 2000.

Como hemos visto en el apartado anterior, no es necesaria la autorización del director de la AEPD para la transferencia internacional de datos cuando el importador cuenta con las medidas de protección suficientes de acuerdo al criterio de la Comisión Europea.

En Estados Unidos, debido a la tendencia del comercio a tener un marcado carácter autorregulador y a la pluralidad de normativa existente (tanto sectorial como federal), no existe una regulación de protección de datos aplicable a todo el país que la comisión europea pueda valorar con el fin de decidir si cumple o no con los requisitos de protección necesarios para la transferencia internacional de datos.

Debido a la ausencia de una regulación de protección de datos unificada, el Departamento de Comercio de Estados Unidos elaboró un documento que contenía unos principios de "puerto seguro" o Safe Harbor, al que las empresas que cumpliesen con dichos principios podrían adherirse. El Acuerdo de Safe Harbor consistía (y consiste) en 7 principios básicos: la notificación (información a los afectados); la opción (posibilidad de oposición de los afectados); la transferencia ulterior a terceras empresas; la seguridad; la integridad de los datos (principios de finalidad y proporcionalidad); y el derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados).[24]

Los principios de Safe Harbor pretendían cumplir con los requisitos exigidos por la normativa europea para la transmisión internacional de datos. Las empresas u

[22] Artículo 44.4 LOPD
[23] Artículo 45.3 LOPD
[24] AEPD. Consultado en: https://www.AEPD.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf

operadores que quisiesen transmitir libremente datos entre la Unión Europea y Estados Unidos, sólo tendría que adherirse a los principios del Safe Harbor manifestando su voluntad ante la Oficina Federal de Comercio y adoptando las medidas necesarias para llevarlos a la práctica.

Juan Carlos Galván Barceló ha definido de una forma muy completa los 7 principios básicos del Safe Harbor:

*" "**Notice"**. Deber de información (o notificación). Las entidades adheridas a Safe Harbor deben informar a los interesados de las finalidades para las cuales han sido recabados sus datos así como de la identificación del Responsable del Fichero, a efectos de poder ejercitar los derechos ARCO. Este principio se encuentra recogido en el artículo 5 de nuestra Ley Orgánica de Protección de Datos de Carácter Personal.*

*"**Choice"**. Corresponde al interesado o afectado el poder decidir acerca de la finalidad y destino de sus datos de carácter personal. Este postulado se corresponde con nuestro consagrado principio del consentimiento del afectado o interesado. (Art. 6 LOPD).*

*"**Transfers to Third Parties"**. Según este principio, sólo será posible la transferencia de datos cuando las entidades o países destinatarios estén suscritos al acuerdo Safe Harbor o sean países miembros de la Unión Europea (sometidos a la Directiva 95/46/CE). Sería algo equivalente al Título V de nuestra Ley Orgánica de Protección de Datos, en relación con los artículos 9 y 12. Se entiende que estas transferencias están sometidas al principio anterior (consentimiento o poder de decisión).*

*"**Access"**. No serviría de nada la información facilitada por el primero de los principios Safe Harbor si el interesado no pudiera hacer efectivos sus derechos. Nos encontramos ante los derechos-obligación recogidos en el Título III de la Ley Orgánica de Protección de Datos, los consabidos derechos ARCO (acceso, rectificación, cancelación y oposición).*

*"**Security"**. Se corresponde plenamente con el artículo 9 de nuestra LOPD, el principio de seguridad de los datos: "adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado". La única cuestión que plantea Safe Harbor en relación con nuestra LOPD, es que el primero habla de "precauciones razonables", pareciendo dejar al libre albedrío del Responsable del Fichero, las medidas a adoptar.*

*"**Data integrity"**. El importantísimo principio de "Calidad de los datos" acuñado por la Directiva 95/46/CE y recogido con precisión en nuestra LOPD, pasa a formar parte de los requisitos de Safe Harbor, aunque no con toda su extensión porque, por ejemplo, no se incluye aquí lo relativo a la cancelación de los datos y su posible conservación.*

*"**Enforcement"**. Este principio se refiere a la concreta aplicación o ejecución de todo lo que conlleva Safe Harbour. Es un principio controvertido por su ambigüedad, que dispone que para garantizar el cumplimiento de los postulados de puerto seguro, deben articularse mecanismos independientes de resolución de conflictos y de*

verificación del cumplimiento de los principios Safe Harbor, con potestad para sancionar, en su caso. En España, estas competencias son asumidas por la Agencia Española de Protección de Datos. En cuanto a Safe Harbor, ese mecanismo de resolución de conflictos brilla por su ausencia".[25]

Finalmente, la Comisión Europea llegó a un acuerdo con el Departamento de Comercio de Estados Unidos por el que vio la luz la "Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

A raíz de la decisión 2000/520/CE de 26 de julio de 2000, se hizo efectiva la libre transmisión de datos entre los exportadores de la Unión Europea y los importadores de Estados Unidos adheridos a los principios del Safe Harbor.

La Sentencia del TJUE de 6 de octubre de 2015 ha anulado la decisión 2000/520/CE de la Comisión Europea, pero ésta no ha sido la primera muestra de rechazo por parte de Europa hacía el sistema de Safe Harbor.

Ya en el año 2004 la Comisión Europea de Justicia elaboró un informe[26] en el que quedaban patentes algunas de las deficiencias del sistema Safe Harbor, que podemos resumir en:

- Falta de transparencia e inteligibilidad de la información proporcionada.
- No se hacía referencia al principio de consentimiento.
- Respecto a las transferencias a terceros, el concepto de "tercero" no siempre quedaba definido.
- El principio del acceso tendía a estar muy difuminado en la práctica, llegando a faltar incluso los datos de contacto.
- La integridad o calidad de los datos tampoco se hacía efectiva correctamente, siendo difícil determinar la adecuación o pertinencia de los datos en relación con las actividades o finalidades previstas.

[25] GALVAN BARCELÓ. 2010. Consultado en : http://www.actualidadlopd.com/2010/10/06/lopd-safe-harbor-%C2%BFgolpe-de-timon-del-derecho-anglosajon/
[26] GALVAN BARCELÓ. 2010. Consultado en : http://www.actualidadlopd.com/2010/10/06/lopd-safe-harbor-%C2%BFgolpe-de-timon-del-derecho-anglosajon/

- El listado de las empresas adheridas a los principios de Safe Harbor estaba desfasado.

III.2.3. Estados Unidos y la Privacidad. Caso Snowden.

Si el sistema de principios de Safe Harbor ya se encontraba en entredicho a raíz de las diferentes deficiencias que éste presentaba, y que se han mencionado en el apartado anterior, en el año 2013 surgió un escándalo que puso en entredicho la protección de los datos en Estados Unidos.

Edward Snowden, un ex agente de la NSA, reveló diversos documentos confidenciales que probaban que Estados Unidos estaba accediendo de forma indiscriminada y masiva a datos protegidos. La NSA recopilaba las listas de llamadas telefónicas, incluidos los números, la hora y la duración de las llamadas. Las organizaciones gubernamentales de Estados Unidos no sólo estaban accediendo a datos relacionados con telecomunicaciones, si no que se recopilaban contenidos de búsquedas electrónicas, de emails y documentos de los usuarios de diferentes empresas.[27]

La revelación de todos estos datos por parte de Snowden (y la consiguiente polémica que ello ha generado), ha hecho que Estados Unidos haya avanzando en el camino de darle al derecho a la privacidad la importancia que se merece.

La Ley que amparaba las injerencias de Estados Unidos en datos protegidos de los ciudadanos era la “Patriotit Act”, concretamente la sección 215. Dicha ley vio la luz a raíz de los atentados del 11S en el año 2001, lo que explica la fuerte injerencia en la privacidad de los ciudadanos, justificada en su momento por motivos de seguridad pública.

En junio de 2015 se aprobó la “USA Fredoom Act”, siendo uno de sus elementos centrales retirar a la NSA la capacidad de almacenar los datos sobre las llamadas telefónicas de los estadounidenses y colocar estos datos en manos de las

[27] EL PAÍS. 2015. Consultado en: http://internacional.elpais.com/internacional/2015/06/02/actualidad/1433277585_519201.html

compañías telefónicas. Sólo se podrá acceder a estos datos caso a caso y previa autorización judicial.[28]

Si bien con la aprobación de la USA Freedom Act Estados Unidos ha dado los primeros pasos para darle más importancia al derecho a la privacidad, esto no ha sido suficiente para el TJUE, que el pasado 6 de octubre de 2015 ha dictado la Sentencia que ha anulado la validez de los acuerdos del Safe Harbor como principios de protección de los datos transferidos internacionalmente desde la Unión Europea

III.2.4. Sentencia del TJUE de 6 de octubre de 2015.

Después de 15 años de libre transferencia de datos entre Europa y las empresas estadounidenses adheridas al acuerdo de Safe Harbor, el TJUE ha dictado una Sentencia el 6 de octubre de 2015, que ha invalidado la decisión 2000/520/CE de la Comisión de 26 de julio de 2000 y por lo tanto el propio acuerdo de Safe Harbor.

La Sentencia referida en el párrafo anterior fue dictada en el asunto C-362/14, a raíz de la cuestión prejudicial planteada por la High Court de Irlanda en el procedimiento seguido entre Maximillian Schrems y el Data Protection Commissioner, con intervención de Digital Rights Ireland Ltd.

El procedimiento se inició el 25 de junio de 2013 por el ciudadano austriaco Maximillian Schrems, usuario de facebook, cuando solicitó al Data Protection Commissioner de Irlanda que prohibiese a Facebook Ireland transmitir sus datos personales a Estados Unidos. La petición del Sr. Schrems se basaba en gran parte en las revelaciones hechas ese mismo año por Edward Snowden acerca del espionaje masivo e indiscriminado llevado a cabo por la NSA.

El Data Protection Commissioner irlandés resolvió la petición del Sr. Schrems alegando que:

[28] EL PAÍS. 2015. Consultado en : http://internacional.elpais.com/internacional/2015/06/02/actualidad/1433277585_519201.html

"no estaba obligado a investigar sobre los hechos denunciados por el usuario, (..) ya que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión 2000/520".[29]

Ante dicha resolución, el Sr. Schrems presentó un recurso ante la High Court irlandesa, que reconoció que:

"el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa. Para que las interceptaciones de comunicaciones electrónicas puedan ser consideradas conformes con esa Constitución, debe aportarse la prueba de que esas interceptaciones tienen carácter selectivo, de que la vigilancia de determinadas personas o de determinados grupos de personas está objetivamente justificada en interés de la seguridad nacional o de la represión de la delincuencia y de que existen garantías adecuadas y comprobables"[30].

Según la High Court, si fuese de aplicación el derecho irlandés sin tener en cuenta la decisión de la Comisión Europea acerca de la validez de los principios de Safe Harbor:

"existen serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, y el comisario habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente"[31].

Como lo que en realidad el Sr. Schrems impugnaba en su recurso era la licitud del régimen de «puerto seguro», el High Court irlandés decidió suspender el procedimiento y plantear dos cuestiones prejudiciales:

"¿está vinculado el Comisario irlandés en términos absolutos por la declaración comunitaria contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta Europea de los Derechos Fundamentales y no obstante lo dispuesto en la Directiva 95/46/CE?; en caso contrario, ¿puede o debe realizar dicho Comisario su propia investigación del asunto a la luz de la evolución de los hechos que han tenido lugar desde que se publicó por vez primera la Decisión 2000/520?".[32]

[29] Sentencia TJUE 6-362/14 de 6 octubre de 2015.
[30] Sentencia TJUE 6-362/14 de 6 octubre de 2015.
[31] Sentencia TJUE 6-362/14 de 6 octubre de 2015.
[32] Sentencia TJUE 6-362/14 de 6 octubre de 2015.

El TJUE resolvió que nada impide que una autoridad de control de un Estado miembro, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

Concretamente la Gran Sala del Tribunal de Justicia declaró que:

"1) El artículo 25, apartado 6, de la de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado"[33].

[33] Sentencia TJUE 6-362/14 de 6 octubre de 2015.

Ahora bien, la Sentencia del TJUE fue más allá y declaró inválida la decisión 2000/520/CE de la Comisión de 26 de julio de 2000, basándose para ello en los siguientes motivos[34]:

- El Tribunal de Justicia observó que la Comisión se limitó a analizar el régimen de puerto seguro sin comprobar si Estados Unidos garantizaba efectivamente, en razón de su legislación interna o de sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en la Unión en virtud de la Directiva. El Tribunal de Justicia señala que las autoridades públicas estadounidenses no están sometidas a dicho régimen puesto que éste únicamente es aplicable a las entidades estadounidenses que se han adherido a él.

- Las exigencias de seguridad nacional, interés público y cumplimiento de la ley de Estados Unidos prevalecen sobre el régimen de puerto seguro, de modo que las entidades estadounidenses están obligadas a dejar de aplicar, sin limitación, las reglas de protección previstas por ese régimen cuando entren en conflicto con las citadas exigencias. El régimen estadounidense de puerto seguro posibilita de ese modo injerencias por parte de las autoridades públicas estadounidenses en los derechos fundamentales de las personas, y la Decisión de la Comisión no pone de manifiesto que en Estados Unidos haya reglas destinadas a limitar esas posibles injerencias ni que exista una protección jurídica eficaz contra éstas.

- Por lo que se refiere a un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión, el Tribunal de Justicia observa que en el Derecho de la Unión una normativa no se limita a lo estrictamente necesario cuando autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior.

- Una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada. Asimismo, una normativa que no prevé posibilidad alguna de que el afectado ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión vulnera el contenido esencial del derecho fundamental a la tutela judicial efectiva, cuando esa posibilidad es inherente a la existencia del Estado de Derecho.

- Finalmente, el Tribunal de Justicia declara que la Decisión de la Comisión de 26 de julio de 2000 priva a las autoridades nacionales de control de sus

[34] Comunicado Prensa TJUE 117/15. 6 de octubre de 2015. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

> facultades, en el supuesto de que una persona impugne la compatibilidad de la Decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas. El Tribunal de Justicia considera que la Comisión carecía de competencia para restringir de ese modo las facultades de las autoridades nacionales de control.

Han sido varias las opiniones que se han vertido a raíz de publicación de la Sentencia y de la declaración de invalidez de la decisión 2000/520/CE. Entre ellas podemos mencionar la de Ricard Martínez:

"Las consecuencias de la sentencia son de una enorme magnitud. Por una parte, se consolida la tendencia apuntada en Costeja respecto de la aplicación de la norma europea a los tratamientos de datos personales en otros países, y reafirma esta idea que adquirirá la condición de norma positiva de aprobarse la Propuesta de Reglamento en su actual redacción. De otra, se avanza en la construcción de un derecho fundamental hoy vacío de contenido de la mano de políticas de privacidad incomprensibles, leyes de seguridad nacional invasivas, y condiciones generales de contratación sencillamente innegociables. Al Tribunal, no le basta con meras declaraciones de cumplimiento, exige una garantía real y efectiva de un derecho profundamente prestacional y altamente exigente".[35]

Enrique Dans también se ha pronunciado acerca de la Sentencia, y la creciente acentuación de las diferencias entre la manera de interpretar la privacidad por la Unión Europea y por Estados Unidos:

"Obviamente, la medida tendrá consecuencias: ante la dificultad de que la administración norteamericana, caracterizada por una brutal y descontrolada hipertrofia de agencias como la NSA, modere sus agresivas prácticas de vigilancia y monitorización, y sobre todo, ante la escasa o nula credibilidad que tendría cualquier anuncio al respecto, las compañías norteamericanas se verán obligadas a plantear que el tratamiento de los datos de sus usuarios se lleve a cabo sin salir de la Unión Europea, como de hecho ya había sido anunciado por alguna empresa como Twitter, que se adelantó a este posible desenlace con un anuncio el pasado abril. No es el fin del mundo para compañías que sin duda tienen los recursos adecuados para poner en marcha estos cambios, pero sin duda subraya el creciente desencuentro entre la forma de entender los derechos de los ciudadanos en Europa y en los Estados Unidos".[36]

[35] MARTÍNEZ MARTÍNEZ. 2015. Disponible en: http://www.bez.es/578211217/Safe-Harbour-y-el-modelo-europeo-de-proteccion-de-datos..html#posicion_2

[36] DANS ENRIQUE. 2015. Disponible en : http://www.enriquedans.com/2015/10/el-safe-harbor-no-era-tan-safe.html

III.2.5. Futuro de las transmisiones internacionales de datos a Estados Unidos.

La Sentencia del TJUE de 6 de octubre de 2015 que ha invalidado los acuerdos de Safe Harbor, ha provocado que automáticamente todas las transferencias internacionales realizadas en base a la decisión 2000/520/CE resulten inválidas.

Se estima que las empresas afectadas por el fin del Safe Harbor superan las 4.500.[37]

Si tenemos en cuenta que, como ya se expuso en el apartado III.2.1, la sanción en España por la transferencia de datos internacionales a países que no otorguen un nivel de protección equiparable al de la LOPD oscila entre 301.000 € y 600.000 €, podemos comprender que la STJUE de 6 de octubre de 2015 puede acarrear importantes consecuencias económicas a las empresas que no regulen sus transferencias internacionales de datos a Estados Unidos.

Las Autoridades europeas de Protección de Datos, reunidas en el grupo de trabajo del artículo 29, no tardaron en reaccionar ante la Sentencia del TJUE y la situación de incertidumbre que se creó a raíz de la misma.

El 19 de octubre de 2015, 18 días después de la publicación de la STJUE, las Autoridades europeas de Protección de Datos publicaron una declaración[38] conjunta en relación con la aplicación de la misma.

En dicha declaración, a mayores de solicitar a las autoridades europeas que se iniciasen conversaciones con las autoridades de EEUU a fin de encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos al territorio de EEUU respetando los derechos fundamentales, se expone lo siguiente:

"Durante este período, las Autoridades de protección de datos consideran que las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes (BCRs) pueden seguir utilizándose. En cualquier caso, esto no impedirá que las Autoridades de protección de datos investiguen casos particulares, por ejemplo, a partir de denuncias, y ejerzan sus poderes con el fin de proteger a las personas.

[37] EL DIARIO. 2015. Disponible en: http://www.eldiario.es/hojaderouter/shortcut/Safe_Harbor-privacidad-proteccion_de_datos-empresas-terminos_y_condiciones_6_456064401.html

[38] AEPD. 2015. Disponible en: http://www.AEPD.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php

Si a finales de enero de 2016 no se ha encontrado una solución adecuada con las autoridades estadounidenses, y en función de la evaluación de las herramientas de transferencia por parte del Grupo de Trabajo, las Autoridades de protección de datos de la UE se comprometen a adoptar todas las medidas necesarias y apropiadas, que pueden incluir acciones coordinadas de aplicación de la ley (enforcement).

En cuanto a las consecuencias prácticas de la sentencia del TJUE, el Grupo de Trabajo considera que está claro que las transferencias procedentes de la Unión Europea a EEUU ya no se pueden enmarcar en la Decisión de Adecuación de la Comisión Europea 2000/520/CE (la llamada "Decisión Puerto Seguro"). En cualquier caso, las transferencias que aún se estén llevando a cabo bajo la Decisión Puerto Seguro tras la sentencia del TJUE son ilegales".[39]

La declaración de las Agencias europeas de Protección de Datos ha supuesto, para todas las empresas afectadas por la invalidez de los acuerdos de Safe Harbor, una importante aclaración de su situación jurídica. Si bien la declaración de 19 de octubre de 2015 se reafirma en la idea de que la Decisión 2000/520/CE es inválida, otorga un plazo hasta finales de enero de 2016 a las empresas afectadas para poder regularizar sus transferencias internacionales de datos a Estados Unidos.

En cuanto a la negociación de un nuevo acuerdo de Safe Harbor, que respete las exigencias plasmadas en la Sentencia de 6 de octubre de 2015 por el TJUE para ser considerado válido, la comisaria europea de Justicia, Vera Jorouva, en declaraciones recogidas por el diario The Wall Street Journal, ha declarado que:

"Existe un principio de acuerdo sobre estos aspectos, pero seguimos discutiendo cómo asegurarnos de que las exigencias del Tribunal se cumplan".

"Jorouva ha explicado que el acuerdo resultante de estas negociaciones deberá establecer límites y condiciones claros para el acceso de las autoridades norteamericanas a los datos de los ciudadanos europeos, una de las cuestiones que el escándalo Snowden puso sobre la mesa. Más tímidamente, ha señalado que una revisión del 'Safe Harbor' también ayudará a que los usuarios de la UE tengan información más transparente sobre lo que las compañías estadounidenses hacen con sus datos".[40]

Mientras no se concreta el cierre de un nuevo acuerdo de principios de Safe Harbor, las empresas que transfieran datos desde la Unión Europea a Estados Unidos (y que lo hagan en virtud de los acuerdos de Safe Harbor invalidados) disponen de un

[39] AEPD. 2015. Disponible en: http://www.AEPD.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php

[40] TICBEAT. 2015. Disponible en: http://www.ticbeat.com/tecnologias/eeuu-la-ue-alcanzan-acuerdo-para-actualizar-el-safe-harbor/

plazo hasta finales de enero de 2016 para decidir si van a esperar al cierre de ese nuevo acuerdo, o si van a adoptar otro tipo de soluciones.

En España las posibles soluciones que se pueden adoptar, para realizar las transferencias internacionales de datos a Estados Unidos de una forma válida, son las siguientes:

"1) Autorización de la Directora de la Agencia Española de Protección de Datos:

Deberá darse cumplimiento a las obligaciones establecidas en la LOPD, y acreditar que han sido obtenidas garantías suficientes respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos (e.j. aportando contrato escrito entre el exportador y el importador de datos en el que consten dichas garantías).

a) Transferencias Internacionales entre responsables de tratamiento: deberán reunir las garantías citadas aquellos contratos celebrados en los términos recogidos en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, y 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la anterior. Dichas decisiones contienen cláusulas contractuales tipo, pudiendo optar los Responsables por uno u otro conjunto de cláusulas, no pudiendo modificarlas ni combinarlas.

b) Transferencias Internacionales desde responsable de fichero a encargado del tratamiento: reunirían dichas garantías aquellos contratos que incluyan las cláusulas contractuales tipo establecidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010.

c) Transferencia Internacional de encargado a subencargado del tratamiento: proporcionarán las garantías adecuadas aquellos contratos que incluyan las cláusulas tipo adoptadas en la resolución de la Agencia Española de Protección de Datos de Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012. Junto con el contrato entre el encargado del tratamiento/exportador de los datos e importador/subencargado del tratamiento, se requerirá el contrato marco entre el responsable del tratamiento y el encargado del tratamiento/exportador de datos en el que aquél autorice la subcontratación y la transferencia internacional de datos.

2) Conforme a la normativa vigente en materia de protección de datos, podrán autorizarse transferencias internacionales entre sociedades/empresas de un mismo grupo multinacional de empresas, siempre que se hubieran adoptado normas internas vinculantes para dichas empresas y exigibles conforme al ordenamiento jurídico español. En este sentido el 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 (en adelante, "RLOPD") establece (art. 70.4 y el Título IX, Capítulo V) el régimen jurídico aplicable a las mismas.

En caso de optar por esta vía deberá tenerse en cuenta los Documentos de Trabajo

elaborados por el Grupo del Artículo 29 relativos al contenido de las normas corporativas vinculantes y al procedimiento previo, que se desarrolla entre los diferentes Estados Miembros implicados para la aprobación de éstas".[41]

A mayores de las soluciones mencionadas cabe recordar que, como ya se expuso en el apartado III.2.1, ciertas transferencias internacionales de datos recogidas en el artículo 34 y en el artículo 66.2 de la LOPD, se encuentran exentas de autorización por el Director de la AEPD.

No podemos obviar que una solución definitiva para muchas empresas sería la de comenzar a situar los datos personales de los ciudadanos europeos en la propia Unión Europea, cesando la transferencia internacional de los mismos a Estados Unidos. Microsoft ha sido de las primeras empresas en tomar esta determinación, anunciando que "*a partir de 2016, los de Redmond ofrecerán sus servicios en la nube desde sus centros de datos instalados en Alemania. Así, la información de sus usuarios no saldrá de las fronteras de la Unión Europea y serán tratados con las garantías de protección comunitarias"*[42].

En vista del plazo concedido por la declaración de 19 de octubre de 2015, pocas empresas han reaccionado hasta el momento para adaptar sus transferencias internacionales de datos a Estados Unidos. Se estima que sólo un 3% de las empresas afectadas han realizado cambios en sus políticas de privacidad.[43]

Probablemente las empresas más afectadas serán, sin embargo*, las pequeñas empresas que, amparadas en el Safe Harbor, gestionaban en Estados Unidos, por ejemplo, servicios en la nube ("Cloud computing"), ya que éstas pueden llegar a mover grandes cantidades de datos por minuto/día y pueden no tener capacidad ni de solicitar una autorización ni de suscribir acuerdos bilaterales en tal sentido.*[44]

III.3. **DERECHO AL OLVIDO**

[41] ECIJA. 2015. Disponible en: http://www.ecija.com/notas-de-prensa/nota-informativa-infografia-soluciones-tras-la-invalidez-de-safe-harbor/
[42] EL DIARIO. 2015. Disponible en: http://www.eldiario.es/hojaderouter/shortcut/Safe_Harbor-privacidad-proteccion_de_datos-empresas-terminos_y_condiciones_6_456064401.html
[43]EL DIARIO. 2015. Disponible en: http://www.eldiario.es/hojaderouter/shortcut/Safe_Harbor-privacidad-proteccion_de_datos-empresas-terminos_y_condiciones_6_456064401.html
[44]JIMÉNEZ DE LA IGLESIA – ARMADA. 2015. Disponible en: http://www.expansion.com/juridico/opinion/2015/10/26/562e880346163fc4438b4593.html

Otra de las Sentencias dictadas por el TJUE, de gran relevancia para la configuración de la privacidad en el ámbito de la Unión Europea, es la de 13 de mayo de 2014 en relación con el derecho al olvido.

Con las nuevas tecnologías, y especialmente con la aparición de internet y de los buscadores electrónicos de contenidos, ha surgido lo que podemos denominar como "memoria digital".

La memoria del ser humano tiene una capacidad limitada, justo al contrario de lo que ocurre con internet, que se ha convertido en un medio que ha revolucionado nuestra forma de vida.

Si tenemos en cuenta el gran flujo de información que hay en internet y la proliferación de dispositivos de guardado masivo de datos, podemos observar que las dimensiones de la "memoria digital" hacen muy difícil que los ciudadanos puedan controlar los datos expuestos acerca de ellos en la red.

El hecho de que determinados datos de los ciudadanos queden fuera de su control en la red y permanezcan fácilmente accesibles a través de los buscadores digitales a pesar del transcurso del tiempo, afecta al derecho a la intimidad, al derecho al honor, al derecho a la protección de datos y al derecho a la propia imagen.

Esta situación choca con nuestro ordenamiento jurídico, en el que se reconoce el derecho al olvido en determinadas situaciones, como pueden ser la cancelación de los antecedentes penales y judiciales de los ciudadanos transcurrido un cierto período de tiempo.

El derecho al olvido pretende dar respuesta a esta situación. Según la AEPD:

"el denominado 'derecho al olvido' es la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque

la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información)".[45]

III.3.1. Derecho al olvido y su relación con los artículos 10.1 y 18.4 de la Constitución Española.

Para comprender el contenido del derecho al olvido debemos atender a dos de los principios que rigen el derecho a la protección de datos personales. Estos principios son el principio del consentimiento y la finalidad de los datos.

La LOPD define el consentimiento en su artículo 3 como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le concierne."*[46].

Debemos distinguir entre las diferentes formas de otorgar el consentimiento por parte de las personas para publicar sus datos en la red. Una primera forma es que la misma persona los publique y luego quiera eliminarlos, revocando así su consentimiento. Otra forma es que un tercero suba los datos sin consultarle al titular de los mismos, y con posterioridad éste quiera eliminarlos. Por último, también puede suceder que sea una administración pública o un medio informativo el que haya publicado la información. En este último caso, aunque la publicación se haya hecho con una base legal, esto no quiere decir que una vez que dicha base legal desaparezca, o la información deje de ser pertinente, deba eliminarse.[47]

La finalidad de los datos también es de suma importancia para comprender el contenido del derecho al olvido. El art. 11.1 LOPD recoge que "*Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado*".[48] *A juicio de SIMÓN CASTELLANO, "el principio de finalidad podría constituir una base sólida para el derecho al olvido digital, al establecer que los datos personales serán*

[45] AEPD. 2015. Disponible en: http://www.AEPD.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php
[46] Artículo 3 LOPD
[47] HERNÁNDEZ RAMOS. 2013. Disponible en: http://catedraseguridad.usal.es/sites/default/files/files/CUADERNO_11_DERECHO%20OLVIDO.pdf
[48] Artículo 11.1 LOPD

eliminados o borrados una vez que estos hayan dejado de ser útiles a la finalidad con la que se registraron".

Por lo tanto, el derecho de finalidad está vinculado al derecho a la cancelación de los datos personales a petición del interesado cuando estos ya no cumplan con la finalidad para la que fueron recabados. Sin embargo, hay que tener en cuenta que no siempre será posible la cancelación de dichos datos.

En muchas ocasiones el mayor problema que surge a la hora de la aplicación del derecho al olvido es su colisión con otros derechos, principalmente con el derecho a la libertad de expresión. El enfrentamiento entre el derecho al olvido y otros derechos fundamentales debe resolverse haciendo una ponderación caso por caso de los derechos en conflicto. Esta es la postura que ha adoptado la AEPD en sus resoluciones (como veremos en los siguientes apartados) y que ha mantenido el TJUE en su Sentencia de 13 de mayo de 2014.

Mario Hernández Ramos, en su artículo "El derecho al olvido digital en la web 2.0" ha realizado las siguientes reflexiones en relación con la ponderación de derechos en conflicto y la jurisprudencia del TC al respecto:

"aunque la Constitución no imponga expresamente límites específicos a un derecho fundamental determinado, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (STC 11/1981, de 8 de abril, FJ 7; respecto del art. 18 CE, STC 110/1984, FJ 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental." (STC 292/2000, de 30 de noviembre, FJ 11). El eventual ejercicio del derecho al olvido debería ser considerado de una forma similar a la ponderación entre derechos fundamentales en conflicto, acudiendo a los criterios utilizados por la jurisprudencia constitucional".[49]

Debemos de tener en cuenta que, al encontrarnos en un estado democrático de derecho, es comprensible que el interés público tenga una gran relevancia a pesar de la importancia que han adquirido los derechos de la personalidad. Según Pere Simón Castellano, para ponderar correctamente el derecho a la libertad informativa frente al derecho al olvido digital, debemos tener en cuenta tres criterios: el interés

[49] HERNÁNDEZ RAMOS. 2013. Disponible en: http://catedraseguridad.usal.es/sites/default/files/files/CUADERNO_11_DERECHO%20OLVIDO.pdf

público actualizado, el estudio del contexto en el que se ha difundido la información y aplicar el principio de proporcionalidad.[50]

Por último, para comprender el contenido del derecho al olvido, debemos referirnos a él como un derecho que se encuentra amparado por la combinación de dos derechos fundamentales, como son el derecho a la privacidad y el derecho a la dignidad de la persona.

El derecho a la privacidad y a la protección de datos ya ha sido analizado en el apartado III.1, no queda ninguna duda de que el derecho al olvido nace intrínsecamente unido a este derecho fundamental dado su contenido.

El otro derecho que debemos analizar es el derecho a la dignidad de la persona y al libre desarrollo de la personalidad, que se encuentra recogido en el artículo 10.1 de la Constitución Española:

"Artículo 10 Constitución Española
10.1 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. (...)"[51]

Si a una persona no se le permite hacer uso de su derecho al olvido digital sobre un determinado contenido de manera injustificada, estaremos atentando sobre su capacidad de determinar libremente su vida y de permanecer en el anonimato.

La conexión entre el derecho a la dignidad de la persona y el derecho a la privacidad no ha surgido exclusivamente a raíz del surgimiento del derecho al olvido digital. La STC 231/1998, de 2 de diciembre, ya relacionaba los derechos recogidos en el artículo 18 de la Constitución con el derecho fundamental reconocido en el artículo 10.1 del mismo cuerpo normativo:

"Hay que recordar que la dignidad humana tiene una conexión inextricable con los derechos de la personalidad, esto es, con el honor, la propia imagen, la intimidad y la protección de los datos personales. En concreto el máximo intérprete constitucional ha detallado que los derechos reconocidos en el art. 18 de la CE aparecen como <<derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda alguna de la dignidad de la persona que reconoce el artículo 10 de la CE>>. De ese modo, los derechos de la personalidad que

[50] SIMÓN CASTELLANO (2015 : 197)
[51] Artículo 10 CE

eventualmente pueden verse afectados por el recordatorio constante de noticias pasadas, están enlazados intrínsecamente a la dignidad humana. De hecho, se les ha catalogado como derechos de libertad y autonomía porque fueron concebidos para garantizar una esfera reservada al individuo frente a la acción de los demás."[52]

Finalmente, no podemos dejar de hacer referencia a la definición que Simón Castellano, referente en la materia, aporta en relación con el derecho al olvido digital, definiendo el mismo:

"como un derecho que exige que los datos de las personas dejen de ser accesibles en la web, por petición de las mismas y cuando estas lo decidan; como un derecho a retirarse del sistema y eliminar la información personal que la red contiene. Más concretamente, se trata de un derecho de la ciudadanía a cancelar y oponerse al tratamiento de sus datos personales cuando estos han dejado de ser útiles o necesarios para el propósito con el que fueron recabados o publicados." [53]

III.3.2. Reconocimiento del derecho al olvido por la AEPD y las Agencias de Protección de Datos Europeas.

La Agencia Española de Protección de Datos ha tenido un papel pionero en el reconocimiento del derecho al olvido[54]. Desde el año 2009 la AEPD ha ido constatando la creciente preocupación de los ciudadanos por eliminar de los motores de búsqueda digitales resultados de búsqueda concernientes a aspectos de su vida privada. La primera resolución de la AEPD en la que se habla del derecho al olvido digital data del año 2007.

Las peticiones realizadas a la AEPD solicitando la eliminación de determinados resultados en los motores de búsqueda digitales, se han realizado basándose en los derechos de oposición y cancelación sobre los datos personales.

Los derechos de oposición y cancelación forman parte de los derechos ARCO que todo ciudadano puede ejercer sobre sus datos personales, como parte del derecho de protección de datos. En concreto el derecho de oposición consiste en el derecho del afectado por el tratamiento de sus datos personales a que éste no se lleve a

[52] SIMÓN CASTELLANO (2015 : 180-181)
[53] SIMÓN CASTELLANO (2015)
[54] SIMÓN CASTELLANO (2015 : 204-221)

cabo o se cese, y el derecho de cancelación consiste en la supresión de dichos datos cuando éstos sean inadecuados o excesivos.

La AEPD, desde un primer momento, ha reconocido la relación entre el derecho al olvido y la dignidad de la persona, como podemos observar en el siguiente extracto de la resolución TD/00771/2009:

"En el caso que nos ocupa 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 Agencia Española de Protección de Datos 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 Ley Orgánica 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".[55]

Hay que destacar la importante labor de la AEPD, que ha sabido identificar y tratar correctamente las solicitudes de cancelación y oposición, sobre resultados aportados por motores de búsqueda digitales, como solicitudes de derecho al olvido. A mayores, la AEPD ha tenido en cuenta para sus resoluciones el principio de consentimiento y la finalidad de los datos, no fallando sistemáticamente a favor de los ciudadanos que presentaban sus reclamaciones, si no que ha realizado un análisis ponderado caso por caso.

En el panorama europeo, el primer órgano que dictó una resolución analizando el derecho al olvido digital fue el Garante per la Protezioni dei Dati Personali (máximo órgano italiano de tutela del derecho a la protección de datos). Por su parte, en Francia, la Commission Nationale de l'informatique et les Libertés, se posicionó en 2009 favorablemente al derecho al olvido.

La AEPD, fue sin embargo la primera que extendió la tutela del derecho al olvido digital a los intermediarios de la red, como pueden ser los motores de búsqueda.

III.3.3. Sentencia del TJUE de 13 de mayo de 2014 y conclusiones del abogado general.

[55] Resolución TD/00771/2009 AEPD

Uno de los motores de búsqueda más utilizados es el de la compañía Google. Debido a su popularidad, las reclamaciones realizadas para ejercer los derechos de cancelación y oposición de datos personales, es decir de ejercer el derecho al olvido, realizadas a este buscador a través de la AEPD fueron muy numerosas.

Google ha recurrido sistemáticamente todas las resoluciones dictadas por la AEPD ante la Audiencia Nacional.

Las resoluciones recurridas por google en relación con la aplicación del derecho al olvido llegaron a ser más de 200[56] cuando, el 27 de febrero del 2012, la Audiencia Nacional planteó, mediante un Auto al TJUE, 9 cuestiones prejudiciales en relación con el alcance de este derecho y con la aplicación del alcance de la Directiva 95/46/CE.

Las partes implicadas en el caso C-131/12, que dio origen a la Sentencia del TJUE de 13 de mayo de 2013, fueron Google Spain, S.L., Google Inc. y por el otro lado la AEPD y D. Mario Costeja González.

Entre las más de 200 resoluciones de la AEPD recurridas por Goggle en relación con el derecho al olvido, la Audiencia Nacional ha realizado las pertinentes cuestiones prejudiciales ante el TJUE sobre la resolución impugnada que resolvía la reclamación de D. Mario Costeja. El hecho de que haya sido la reclamación de D. Mario la “seleccionada” por la Audiencia Nacional, probablemente tenga relación con que ésta estaba basada en un caso en el que los datos del reclamante habían sido publicados legítimamente por orden del Ministerio de Trabajo y Asuntos Sociales, es decir por un organismo público.

La AEPD, de hecho, desestimó la reclamación del Sr. Costeja en relación al periódico “La Vanguardia”, en la que se solicitaba que éste eliminase datos referentes a una subasta realizada hacía años, entendiendo que dicha información estaba legalmente justificada.

Sin embargo, la AEPD sí entendió que Google debía desindexar la información que afectaba a la subasta de los bienes del Sr. Costeja de sus resultados de búsqueda, puesto que en este caso la legitimación no sería válida al haber transcurrido varios

[56] URIA. 2014. Disponible en: http://www.uria.com/documentos/publicaciones/4370/documento/fe04.pdf?id=5584

años desde la celebración de la referida subasta, al afectar al derecho a la dignidad humana de D. Mario.

Una de las cuestiones controvertidas de dicha resolución de la AEPD es la aplicación territorial de la LOPD a Google, a pesar de que dicha compañía tiene su sede principal en Estados Unidos. La base para considerar que la LOPD es aplicable en este caso, la encontramos en el artículo 2 del referido cuerpo normativo:

"Artículo 2 Ámbito de aplicación

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito".[57]

La AEPD lleva considerando años a través de diversas resoluciones que:

"aun cuando la empresa no tenga su matriz en España, cuenta con un establecimiento en nuestro país vinculado a su actividad y utiliza medios situados en territorio español. De igual modo, ha considerado que la actividad del buscador, cuando tiene por objeto informaciones relativas a personas físicas identificadas o identificables, constituye un "tratamiento de datos" cuyo responsable no puede ser otro que la empresa que lo gestiona*".*[58]

Pues bien, teniendo en cuenta todos estos precedentes, la Audiencia nacional, al amparo del artículo 267 del TFUE, realizó al TJUE 9 cuestiones prejudiciales para resolver la impugnación realizada por Google Inc. y Google Spain, S.L. a la resolución de la AEPD de 30 de julio de 2010.

[57] artículo 2 LOPD
[58] AEPD. 2014. Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/may_14/NP_STJUE_derecho_olvido.pdf

Las cuestiones prejudiciales realizadas por la Audiencia Nacional pueden dividirse en tres grandes bloques[59]:

1. La aplicación territorial de la Directiva de protección de datos 95/46/CE conforme a los criterios previstos en su artículo 4 y, por consiguiente, de la ley que la incorpora en España, la LOPD, en su artículo 2.1, y el impacto del artículo 8 de la Carta de los Derechos Fundamentales de la UE.
2. El papel de responsable del tratamiento respecto de las actividades realizadas por el buscador a efectos de la Directiva 95/46/CE.
3. El alcance de los derechos de cancelación y oposición en relación con el derecho al olvido.

Si bien como ya se ha adelanto en el conjunto del presente trabajo, el TJUE se posicionó a favor del reconocimiento del denominado derecho al olvido, el abogado general Sr. Niilo Jääskinen se pronunció de una forma desfavorable al mismo en sus conclusiones.

Con respecto al primer grupo de cuestiones prejudiciales planteadas por la Audiencia Nacional, el abogado general reconoció la aplicación de la Directiva 95/46/CE a Google. La base para dicha decisión, es la consideración de que Google utiliza su sede en España con motivo de obtener lucro mediante sus actividades publicitarias, lo que haría que le sea sin duda aplicable la LOPD.

En palabras del abogado general Sr. Niilo Jääskinen:

"Se lleva a cabo tratamiento de datos personales en el marco de las actividades de un "establecimiento" del responsable del tratamiento, en el sentido del art. 4, apartado 1, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (LA LEY. 98204/1995), 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, cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, con el fin de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado".[60]

[59] URIA. 2014. Disponible en: http://www.uria.com/documentos/publicaciones/4370/documento/fe04.pdf?id=5584
[60] Conclusiones abogado general TJUE caso c-131/12, de 26 de junio de 2013.

Con respecto al segundo grupo de cuestiones prejudiciales, el abogado general considera en su informe que si bien se puede considerar que un motor de búsqueda de internet trata datos personales, éste no sería responsable de los mismos mientras no contravenga las peticiones del editor de la página web desde la que los indexa:

"Un proveedor de servicios de motor de búsqueda en Internet cuyo motor de búsqueda localiza información publicada o incluida en Internet por terceros, la indexa automáticamente, la almacena con carácter temporal y, por último, la pone a disposición de los usuarios de Internet, "trata" datos personales, en el sentido del art. 2, letra b), de la Directiva 95/46 cuando esta información contiene datos personales. Sin embargo, no se puede considerar al proveedor de servicios "responsable del tratamiento" de tales datos personales, en el sentido del art. 2, letra d), de la Directiva 95/46, a excepción de los contenidos del índice de su motor de búsqueda, siempre que el proveedor del servicio no indexe o archive datos personales en contra de las instrucciones o las peticiones del editor de la página web"[61].

Por último, y respondiendo al tercer grupo de cuestiones prejudiciales planteadas, el abogado general considera que se estaría atentando gravemente contra la libertad de expresión sí se obliga al motor de búsqueda a eliminar la información indexada:

"Los derechos de cancelación y bloqueo de datos, establecidos en el art. 12, letra b), y el derecho de oposición, establecido en el art. 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas web de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido".[62]

La Sentencia dictada por el TJUE, se ha apartado de las conclusiones del abogado general en los dos últimos grupos de cuestiones prejudiciales planteadas por la Audiencia Nacional.

En relación con el primer grupo de cuestiones prejudiciales, el TJUE coincide con el abogado general en que el establecimiento en España de Google está directamente ligado a las actividades de promoción y venta de espacios publicitarios. Estas actividades resultan elementos muy importantes para la rentabilidad del motor de búsqueda de Google Inc, por lo que la Directiva 95/46/CE y la LOPD, serían de total aplicación territorial al buscador.

[61] Conclusiones abogado general TJUE caso c-131/12, de 26 de junio de 2013.
[62] Conclusiones abogado general TJUE caso c-131/12, de 26 de junio de 2013.

En palabras del TJUE:

"El art. 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro".

Esta resolución del TJUE, acerca de considerar aplicable la directiva 95/46/CE a las empresas que tengan establecimientos en países de la Unión Europea dedicados a la promoción y venta de espacios publicitarios (o otras actividades similares), es sumamente importante y ha provocado que muchas empresas extranjeras que hasta la fecha no consideraban que les fuese de aplicación dicha Directiva, tenga que adaptarse a la nueva situación.

Con respecto al segundo grupo de cuestiones prejudiciales planteadas, el TJUE considera que los gestores de búsqueda realizan un efectivo tratamiento de los datos personales que indexan, y que además son responsables de los mismos. Así concluye que:

"El art. 2, letras b) y d), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de 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 art. 2, letra b), cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse "responsable" de dicho tratamiento, en el sentido del mencionado art. 2, letra d)".

Por último, con respecto al tercer bloque de cuestiones prejudiciales planteadas, el TJUE volvió a apartarse de las conclusiones del abogado general, reconociendo que los gestores de búsqueda deben eliminar de la lista de resultados de búsqueda del nombre de una persona, los resultados que vulneren su derecho al olvido. Para proceder a dicha eliminación deben ponderarse los derechos a la libertad de expresión y el derecho a la privacidad del afectado, teniendo siempre en cuenta el

interés general.

El contenido indexado puede estar legalmente amparado y ello no implica que no se deba eliminar la referencia al mismo al buscar a una determinada persona por su nombre.

Así, en palabras del TJUE:

"Los arts. 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita. Los arts. 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los arts. 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate"[63].

Lo más polémico de la decisión del TJUE, es el hecho de que se deje a los buscadores digitales la decisión de decidir en primera instancia que peticiones relacionadas con el derecho al olvido deben atender y cuáles no.

En relación con este extremo, el despacho Uría Menéndez publicó que:

"Dejando al margen la existencia de criterios para realizar la ponderación de los intereses en juego y, por ello, la dificultad de realizarla, lo sorprendente es que se

[63] Sentencia TJUE de 13 de mayo de 2014. Caso C-131/12.

atribuya al buscador la responsabilidad de realizar esta ponderación y que deba hacerlo de forma independiente a la que realice la fuente original. Y es sorprendente porque no solo es el que peor está situado para realizar este juicio, sino porque tampoco es plenamente congruente con el régimen de responsabilidad de los intermediarios de servicios de la sociedad de la información que pivota sobre el concepto del «conocimiento efectivo», «conocimiento efectivo» que está vinculado a la ilicitud de los datos o a que se hubiera declarado la existencia de la lesión, lo cual parece que debería corresponder a la autoridad de control de protección de datos o a los jueces".[64]

III.3.4. Consecuencias de la Sentencia del TJUE de 13 de mayo de 2014.

La primera consecuencia lógica que tenemos que analizar en relación con la Sentencia del TJUE, es la aplicación de la misma por parte de la Audiencia Nacional para resolver el procedimiento entre Google Inc. y Google Spain por el que impugnaron la resolución de la AEPD.

La Audiencia Nacional dictó Sentencia[65] el 23 de enero de 2014 confirmando los criterios estipulados por el TJUE, y confirmando la resolución de la AEPD. En líneas generales la Sentencia confirma que:

"(i) el tratamiento de datos previo a la indexación que realizan los motores de búsqueda les hace responsables del tratamiento de datos personales, según el artículo 2 de la Directiva; que
(ii) la normativa española le es de aplicación por tener Google una filial establecida en España (Google Spain) y estar la actividad de esta íntimamente ligada a la de la matriz en Estados Unidos; que
(iii) la libertad de información se ve garantizada por la subsistencia de la información en la fuente, es decir, en el sitio web donde se publica la información; que
(iv) se entiende que Google no ve vulnerado su derecho a la libertad de empresa; y, por último, que
(v) el "derecho al olvido" aplicará cuando los resultados generados por una búsqueda no tengan interés público y teniendo en cuenta la fecha de publicación de la información, entre otros factores".[66]

[64] URIA. 2014. Consultado en: http://www.uria.com/documentos/publicaciones/4370/documento/fe04.pdf?id=5584
[65] SAN 5219/2014 de 29 de diciembre de 2014.
[66] ABANLEX. 2015. Consultado en: https://www.abanlex.com/2015/01/la-audiencia-nacional-implementa-en-espana-la-sentencia-del-tjue-sobre-derecho-al-olvido/

Independientemente de la aplicación por la Audiencia Nacional de la Sentencia del TJUE de 13 de mayo de 2014 reconociendo el derecho al olvido al caso del Sr. Costeja, han surgido numerosas dudas de cómo puede aplicarse el contenido de la misma.

Las Autoridades Europeas de Protección de Datos, reunidas en el Grupo del artículo 29, han publicado con posterioridad a la STJUE una serie de recomendaciones para la correcta aplicación de lo dispuesto en ella.

Las directrices desarrolladas por el grupo del artículo 29, y que contienen los criterios interpretativos comunes a seguir en toda Europa, son 25, pero la AEPD ha resumido en una nota de prensa[67] publicada el 28 de noviembre de 2014 las más relevantes:

- Responsabilidad de los motores de búsqueda: Se recuerda que en virtud de la Sentencia de 13 de mayo de 2014, el TJUE consideró que los motores de búsqueda realizan un efectivo tratamiento de los datos personales. La consecuencia inmediata de esta afirmación, es que los motores de búsqueda digitales deben respetar los derechos de cancelación y oposición y por lo tanto el derecho al olvido. A mayores, la consideración de responsables del tratamiento conlleva una serie de obligaciones recogidas en la normativa europea y en la LOPD que los motores de búsqueda deben cumplir.

- Análisis caso por caso: Las Autoridades Europeas de Protección de Datos se centran en resaltar lo ya reseñado hasta ahora, que uno de los aspectos más importante del reconocimiento al derecho al olvido es la ponderación caso por caso de aspectos como la finalidad de los datos y el interés general en el acceso a la información.

Los motores de búsqueda suponen la forma más habitual de acceso a páginas web y resulta preocupante que los resultados vertidos por los mismos puedan realizar fácilmente la configuración del perfil de un individuo, que es precisamente lo que se pretende evitar con el derecho a la protección de datos. Cabe recordar que los

[67] AEPD. 2014. Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/nov_14/141128_NP_AEPD_Aplicacion_Sentencia_TJUE.pdf

intereses económicos de los buscadores digitales nunca pueden prevalecer a derechos tan importantes como el desarrollo personal o el derecho a la privacidad.

- No se elimina información: El Grupo de Trabajo del artículo 29 destaca que la STJUE en ningún momento dice que el ejercicio de los derechos de cancelación y oposición deba implicar que la página original donde se encuentra la información (o la propia información) deban ser suprimidas, si no que sólo afecta a los resultados obtenidos en las búsquedas hechas mediante el nombre de la persona afectada.

- Libertades de expresión e información: Para aquellos que se preocupan por la injerencia del derecho al olvido en el derecho a la libertad de expresión o el derecho a la libertad de información, las Autoridades Europeas recuerdan que la ponderación se realiza caso por caso teniendo en cuenta el interés público. Por ejemplo, cuando se trate de información figuras públicas la que pretende ser eliminada de los resultados de búsqueda, ésta no podría ser eliminada.

- Ejercicio de derechos: Se reseña también que el ejercicio al derecho al olvido por parte de los afectados puede realizarse tanto directamente frente a los motores de búsqueda, como simultánea o alternativamente frente al sitio original donde se encuentren los contenidos afectados. El procesamiento de datos realizado por los motores de búsqueda y los editores web es totalmente diferenciado.

Al respecto, cabe recordar que el procedimiento que dio lugar a la STJUE proviene de la impugnación de una resolución en la que no se reconocía el derecho al olvido frente al sitio web pero sí frente al motor de búsqueda.

- Buscadores internos: Muchas páginas webs tienen buscadores que sólo afectan al contenido de las mismas. Cuando nos encontramos ante este tipo de motores de búsqueda internos, no podemos establecer un perfil completo de la persona cuyos datos resultan afectados, por lo que esta situación queda fuera del ámbito de la sentencia del TJUE.

- Ámbito de aplicación: El grupo de trabajo del artículo 29 recuerda que:

"limitar la eficacia a los dominios europeos basándose en que los usuarios tienden a acceder a través de dominios nacionales no puede considerarse un medio suficiente para garantizar satisfactoriamente los derechos de los interesados. En la práctica, ello implica que la exclusión debe también ser eficaz en todos los dominios relevantes, incluidos los ".com" lo cual abarca, en todo caso, aquellos que sean

accesibles desde el territorio europeo".[68]

- Política de avisos: Algunos buscadores, entre ellos google, cuando un usuario realiza una búsqueda en la que la lista de resultados puede no estar completa por la eliminación de algunos de ellos en base a la aplicación del derecho al olvido, avisan a sus usuarios de la siguiente manera:

"Es posible que algunos resultados se hayan eliminado de acuerdo con la ley de protección de datos europea".

Según las recomendaciones de las Autoridades Europeas de Protección de Datos: "*Esta práctica sólo puede ser aceptable si la información se ofrece de tal manera que los usuarios no puedan deducir, en ningún caso, que una persona concreta ha solicitado la retirada de ciertos resultados asociados a su nombre*".

- Comunicación a terceros: Algunos buscadores antes de desindexar los contenidos que pueden perjudicar el derecho al olvido, comunican a los responsables de la página web en la que se encuentran los contenidos afectados que éstos van a dejar de ser accesibles para determinadas búsquedas. Las Autoridades Europeas de Protección de Datos manifiestan en relación con esta práctica que: *"dado que los buscadores no reconocen a los editores un derecho a ser indexados ni a un trato equitativo, no existe base legal que ampare dicha comunicación. Únicamente se considera justificada la realización de contactos previos cuando sea necesario recabar información adicional para tomar la decisión".*

- Transparencia: La mayoría de la gente en la actualidad utiliza motores de búsqueda para el acceso a páginas web. Los criterios sobre la indexación de las páginas web que siguen los diferentes buscadores de contenidos digitales no son muy claros, a pesar de que para muchos editores resultan claves. El Grupo de Trabajo del artículo 29 considera necesaria la transparencia en este sentido y: "*Las Autoridades europeas instan a los buscadores a que hagan públicos los criterios de exclusión que están aplicando y que faciliten estadísticas detalladas y anonimizadas sobre los tipos de casos en los que han aceptado o rechazado las correspondientes solicitudes*".

[68] AEPD. 2014. Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/nov_14/141128_NP_AEPD_Aplicacion_Sentencia_TJUE.pdf

Después de que haya transcurrido ya más de un año y medio desde la Sentencia del TJUE mediante la que se fijaron los límites del derecho al olvido, podemos hacer una valoración de cómo ha evolucionado el número de solicitudes de retirada de resultados de búsqueda a los buscadores digitales.

Google, el buscador más relevante a nivel mundial y europeo, y que fue parte del caso C-131/12, ha implementado correctamente un sistema para atender las solicitudes de derecho al olvido mediante un formulario en su página web intuitivo y en el que se da a los ciudadanos toda la información necesaria acerca del mismo.

A mayores de lo requerido legalmente, Google informa a través de su sitio web "http://www.google.com/transparencyreport/removals/europeprivacy/" de las solicitudes de retirada de resultados recibidas desde el lanzamiento oficial del proceso de retirada, y el número aceptado y rechazado de las mismas.

A fecha de 3 de diciembre de 2015, el número total de solicitudes recibidas por Google en relación al ejercicio del derecho al olvido es de 351.857, afectando las mismas a un total de 1.245.422 URL, de las cuales sólo se ha retirado el 42.1%.

Si observamos los datos por países, en España el número total de solicitudes es de 33.458, comprendiendo éstas la solicitud de retirada de104.463 URL, de las cuales Google ha retirado el 37,3%.

La publicación de estos datos supone un auténtico ejercicio de transparencia por parte de Google, y en contra de lo que parte de la doctrina preveía, como Simón Castellano Pere al afirmar que *"Además, el tamaño sí importa en la medida que tal cantidad de reclamaciones que en caso de duda razonable y con la mesa llena de expedientes, lo coherente es que el buscador decida desindexar la información"*[69], el porcentaje de URL retiradas no es alarmante ni hace pensar que éstas se estén retirando por sistema.

Sin embargo, sí que hay que tener en cuenta que aunque el Grupo de trabajo del artículo 29 dio unas directrices para la correcta aplicación del derecho al olvido, el papel de decidir que solicitudes se aceptan y cuáles no en relación con el mismo está recayendo en los motores de búsqueda. Simón Castellano, en relación con esta situación ha afirmado que:

[69] SIMÓN CASTELLANO. (2015 : 166).

"Otorgar a los buscadores el papel interpretativo para ponderar derechos fundamentales nos parece un error de gran calado, tanto desde la óptica de las garantías de los derechos como desde la óptica de la arquitectura red. (...) El Consejo Asesor de Google puede equipararse así a un falso tribunal del derecho al olvido digital, cuya actividad pone en cuestión la neutralidad de internet".[70]

Por otro lado, no podemos olvidar que existen más motores de búsqueda que Google, y que no todos cuentan con los medios económicos necesarios para costear un equipo jurídico que revise las solicitudes de derecho al olvido recibidas y decida cuales se aceptan y cuáles no.

III.3.5. Sentencia del TS.

El pleno de la Sala de lo Civil del TS ha dictado una Sentencia el pasado 15 de octubre de 2015, en la que se interpreta el alcance del derecho al olvido en relación con la información contenida en las hemerotecas digitales[71].

El origen del procedimiento que dio lugar a la Sentencia del TS fue una reclamación realizada por dos ciudadanos que vieron como una hemeroteca digital, con motivo de la digitalización de las noticias del periódico al que pertenecía, publicaba una serie de noticias acerca de ellos.

Dichas noticias, consistían en la difusión de unos hechos delictivos que habían tenido lugar hace más de 20 años.

El Juzgado de Primera Instancia y la Audiencia Provincial estimaron la petición de los ciudadanos relacionada con la supresión de sus datos personales de dichas noticias, y con el reconocimiento de una indemnización por los daños causados por el periódico.

El TS ha revocado en parte la Sentencia de la Audiencia Provincial, aunque ha realizado la adecuada ponderación de intereses, considerando desproporcionado el hecho de que desde cualquier buscador de internet se pudiese acceder a la información. En palabras del TS:

---

[70] SIMÓN CASTELLANO. (2015 : 306-307)
[71] NOTICIAS JURÍDICAS. 2015. Disponible en: http://noticias.juridicas.com/actualidad/noticias/10588-primera-sentencia-del-ts-sobre-el-derecho-al-olvido:-si-los-interesados-lo-solicitan-la-informacion-obsoleta-sobre-personas-sin-relevancia-publica-puede-no-ser-buscable/

" Pero la licitud del tratamiento de los datos personales no exige solamente su veracidad y exactitud, sino también su adecuación, pertinencia y carácter no excesivo en relación con el ámbito y las finalidades para las que se haya realizado el tratamiento (art. 6.1.d de la Directiva y 4.1 LOPD). Y esos requisitos no concurren en un tratamiento de estos datos personales en que una consulta en un motor de búsqueda de Internet que utilice sus nombres y apellidos permita el acceso indiscriminado a la información más de veinte años después de sucedidos los hechos, y cause un daño desproporcionado a los afectados.

Tratándose de personas sin relevancia pública y careciendo de interés histórico que la información aparezca vinculada a dichas personas cuando se hace una búsqueda general en Internet utilizando como palabras clave sus nombres y apellidos, el daño es tan desproporcionado que no resulta amparado por el ejercicio de la libertad de información que supone la hemeroteca digital del diario (y el tratamiento en ella de datos personales que permita su indexación por los motores de búsqueda de Internet), que, como se ha dicho, tiene una importancia secundaria respecto de la publicación actual en el diario de las noticias que van sucediendo o que se van conociendo"[72].

A pesar del anterior razonamiento, el TS revocó en parte la Sentencia de la AP.

El TS entiende que el periódico debía de haber puesto los medios necesarios para evitar que los resultados de su hemeroteca, que contenían los datos personales de los demandantes, fuesen indexados por los motores de búsqueda. Sin embargo, lo que no se puede pedir es que la hemeroteca elimine de su motor de búsqueda interno los resultados, puesto que esto afectaría al derecho de libertad de expresión e información.

En definitiva, lo que el TS viene a decir, es que uno no puede configurarse *"un pasado a medida"* a través del ejercicio del derecho al olvido[73].

El fallo de la STS de 15 de octubre de 2015 recoge lo siguiente:

"La consecuencia de lo expuesto es que debe estimarse en parte el recurso de casación y revocar los pronunciamientos relativos a la supresión de los datos personales en el código fuente y del nombre, apellidos o incluso iniciales, y a la prohibición de indexar los datos personales para su uso por el motor de búsqueda interno de la hemeroteca digital.

Procede mantener los pronunciamientos declarativos y los demás pronunciamientos de condena, bien entendido que cuando el fallo de la sentencia del Juzgado de Primera Instancia, asumido por la Audiencia Provincial, declara la ilicitud de la "difusión" de la noticia y condena a Ediciones El País a cesar en su

[72] STS 545/2015 de 15 octubre 2015.
[73] DERECHO OLVIDO. 2015. Disponible en: http://www.derechoolvido.es/sentencia-del-tribunal-supremo-en-un-caso-de-derecho-al-olvido/

"difusión", se está refiriendo exclusivamente al tratamiento de los datos personales incluidos en la noticia tal como se está haciendo en la hemeroteca digital, esto es, permitiendo su indexación por los motores de búsqueda de Internet.

Los demás pronunciamientos se mantienen, en concreto la obligación de Ediciones El País de instalar códigos o instrucciones en la página web que impidan la indexación y archivo de los datos personales de las personas demandantes en las bases de datos de los motores de búsqueda de Internet, la indemnización por los daños causados como consecuencia de la intromisión ilegítima en el honor y la intimidad por el tratamiento de los datos personales sin respetar las exigencias derivadas del principio de calidad de los datos, en lo relativo a su pertinencia, adecuación y proporción en relación a los fines para los que se hizo la recogida y el tratamiento de tales datos, y la prohibición de que en la publicación de cualquier noticia que se refiera a este proceso se incluyan datos que puedan identificar a las personas demandantes, como sus nombres, apellidos o iniciales"[74].

III.3.6. Inclusión del derecho al olvido en la Reforma de la Directiva 95/46/CE.

La Directiva 95/46/CE va a ser reformada mediante la publicación de un nuevo reglamento que regule el Derecho a la Protección de Datos en la Unión Europea. El procedimiento para la reforma de dicha Directiva se inició en el año 2010 por la Comisión Europea.

Han sido muchos los borradores[75] que se han propuesto y discutido a lo largo de estos 5 años. En todos los borradores de reforma de la Directiva 95/46/CE se ha contemplado la inclusión del derecho al olvido, si bien en varios de ellos no quedaba suficientemente clara la responsabilidad de los motores de búsqueda digitales en relación con el mismo.

Ha sido el 15 de junio de 2015 cuando los ministros europeos de Justicia han cerrado un acuerdo político sobre el reglamento de protección de datos personales, que reconoce el derecho al olvido en la misma extensión que lo hizo la Sentencia del TJUE de 13 de mayo de 2014. Tal y como recogió la versión digital del periódico El Mundo:

""Estamos ante algo muy importante, ya que el nuevo reglamento dará a todos los ciudadanos de la Unión un mayor control de todos sus datos. Ahora podrán pedir el

[74] STS 545/2015 de 15 de octubre de 2015.
[75] SIMÓN CASTELLANO (2015 : 300-301)

borrado de sus datos en internet", dijo el ministro letón de Justicia, Dzintars Rascnasc, cuyo país ocupa la presidencia de turno de la UE hasta finales de mes"[76].

III.3.7. Derecho al olvido en el common law.

En los países de tradición jurídica del common law la Sentencia de 13 de mayo de 2014 no ha sido bien recibida, debido en parte a la diferente comprensión del derecho a la privacidad que existe en éstos con respecto a los países de tradición jurídica continental.

Un ejemplo de la diferente visión[77] que existe con respecto al derecho al olvido, lo podemos encontrar en el sistema de difusión de los expedientes judiciales. En países que siguen la tradición del Common Law como Estados Unidos y Canadá, los expedientes judiciales son considerados registro público al primar en todo caso el interés general de los ciudadanos a conocer el contenido de los mismos.

En Estados Unidos son legales las bases de datos digitales que difunden antecedentes penales y determinadas resoluciones judiciales de modo íntegro. En el caso de las resoluciones federales éstas se publican siempre, y en el de las resoluciones estatales se protegen determinados casos (menores de edad) o determinados datos (dirección).

En Canadá se distingue entre el acceso convencional a los expedientes judiciales y el acceso digital, en él que existe una mayor protección de los datos.

Cabe reseñar que en el Reino Unido no se da este supuesto de considerar como registro público los expedientes judiciales. La diferencia entre Reino Unido y los demás países del Common Law se puede justificar en la brecha transatlántica.

Sin embargo, no son pocas las voces que en el Reino Unido se han alzado totalmente en contra del reconocimiento al derecho al olvido digital. En un país cuya tradición civilista es muy distinta a la continental con respecto al derecho a la privacidad, difícilmente se puede entender que predomine éste último frente al derecho a la información y a la libertad de expresión.

---

[76] EL MUNDO. 2015. Disponible en: http://www.elmundo.es/tecnologia/2015/06/15/557e718646163f73038b456b.html

[77] SIMÓN CASTELLANO (2015 : 294-296)

Una de las protestas más destacadas fue la del periódico británico BBC, que ha actuado frente a la Sentencia del TJUE de 13 de mayo de 2014 de la siguiente manera:

"David Jordan jefe de Políticas de Editorial de la BBC, afirmó que en su compañía se "siente que algunos de sus artículos han sido eliminados erróneamente". Un malestar que ha desembocado en la decisión de publicar la lista de los 46 -hasta ahora- enlaces eliminados que le afectan de manera directa a la par que aprovechan para afirmar que el "derecho al recuerdo" no debería caer en un segundo plano para primar de manera tan clara el derecho al olvido recogido por la sentencia del Tribunal de Justicia de la Unión Europea en el "caso Costeja". Una lista que irán actualizando a medida que tanto Google como el resto de motores de búsqueda siga cancelando enlaces que apunten hacia su web. La tarea de creación de un directorio de este tipo resulta muy sencillo para un medio como la BBC debido el propio protocolo de actuación de los motores de búsqueda: cuando Google elimina un enlace en su página de resultados notifica de tal decisión al medio responsable de la publicación del mismo. Es decir, cada vez que Google acepta una solicitud de cualquier ciudadano sobre el derecho al olvido, desde el motor de búsqueda se avisa de ello a la BBC (o cualquier otro medio al que afecte el enlace que se suprimirá). Esta notificación será utilizada a partir de ahora para actualizar un polémico listado"[78].

III.4. CONSERVACIÓN DE DATOS

El 8 de abril de 2014, el TJUE ha dictado una Sentencia (en el marco de los asuntos C-293/12 y C-594/12) que ha supuesto que la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, se haya declarado inválida.

La declaración de invalidez de la directiva 2006/24/CE ha supuesto una situación sin precedentes en el ordenamiento jurídico de nuestro país. Nunca antes se había dado el caso de que se invalidase una Directiva Europea, cuya transposición da origen a una Ley Española.

[78]DERECHO OLVIDO. 2014. Disponible en: http://www.derechoolvido.es/la-bbc-decide-publicar-su-lista-de-enlaces-eliminados-por-el-derecho-al-olvido/

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, es el resultado de la transposición de la Directiva 2006/24/CE en nuestro país.

La finalidad tanto de la Directiva 2006/24/CE, como de la Ley 25/2007, de 18 de octubre, de conservación de datos, es la de conservar los datos tratados por las compañías de telecomunicaciones en las comunicaciones electrónicas. De estos datos se excluye el contenido de las comunicaciones.

III.4.1. Directiva 2006/24/CE y Ley 25/2007, de 18 de octubre, de conservación de datos.

La Directiva 2006/24/CE, surgió en un contexto en el que tras los atentados terroristas del 11M en Madrid y los atentados terroristas de julio de 2005 en Londres, se constató que los medios telemáticos habían sido clave para identificar a los responsables de ambas masacres.

En esa situación de preocupación por la seguridad pública, nació la Directiva 2006/24/CE, cuyo objetivo principal fue:

"armonizar las disposiciones de los Estados miembros sobre la conservación de determinados datos generados o tratados por los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Con ella se pretende así garantizar la disponibilidad de esos datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como la delincuencia organizada y el terrorismo. Así, la Directiva establece que dichos proveedores deberán conservar los datos de tráfico y de localización, así como los datos relacionados necesarios para identificar al abonado o al usuario. En cambio, no autoriza la conservación del contenido de la comunicación ni de la información consultada".[79]

En todo momento quedaron fuera del ámbito de la Directiva los contenidos de las comunicaciones electrónicas. A pesar de esto, la Directiva resultaba muy invasiva en relación con el derecho a la privacidad y a la protección de datos, puesto que siguiendo las indicaciones de la misma se recogían los datos personales sobre las

[79] Nota de prensa del TJUE de 8 de abril de 2014. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

comunicaciones electrónicas de las personas sin ningún tipo de filtro y amparándose sólo en que éstas utilicen un medio tecnológico para comunicarse.

La transposición de la Directiva 2006/24/CE, tuvo lugar en España en el año 2007 a través de la Ley 25/2007, de 18 de octubre:

"Artículo 1 Objeto de la Ley

***1.** Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.*

***2.** Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.*

***3.** Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas"*[80].

En la Ley 25/2007, de 18 de octubre, se fija un límite de 12 meses para la conservación de los datos (encontrándose este plazo entre los 6 y los 24 meses previstos en la Directiva 2006/24/CE. Así mismo, la Ley Española no aporta una definición de lo que se entiende por delitos graves, lo que en la práctica ha causado numerosos problemas.

Por otra parte, el hecho de que esos datos se conserven en virtud de la Directiva y que los jueces nacionales sepan que las teleoperadoras tienen la obligación de conservarlos al menos durante 12 meses, ocasiona frecuentemente que los mismos se soliciten apelando al deber de colaboración judicial recogido en la LOPD. El fin de la Ley de conservación de los datos, concebida exclusivamente para la persecución de delitos graves, se ve constantemente vulnerado al emplearse los datos conservados incluso en procedimientos civiles.

[80] Artículo 1. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

III.4.2. STJUE de 8 de abril de 2014.

La STJUE de 8 de abril se dictó en el seno de los casos C-392/12 y C-594/12. La High Court irlandesa y el Verfassungsgericjtshof alemán, solicitaron al TJUE que examinase la validez de la Directiva 2006/24/CE.

Los antecedentes de hecho de la Sentencia son los siguientes:

"*La High Court (Tribunal Superior de Irlanda) y el Verfassungsgerichtshof (Tribunal Constitucional de Austria) solicitan al Tribunal de Justicia que examine la validez de la Directiva, en particular a la luz de dos derechos fundamentales garantizados por la Carta de los Derechos Fundamentales de la Unión Europea: el derecho fundamental al respeto de la vida privada y el derecho fundamental a la protección de datos de carácter personal.*

La High Court debe pronunciarse sobre un litigio entre la sociedad irlandesa Digital Rights y las autoridades irlandesas relativo a la legalidad de medidas nacionales sobre la conservación de datos referentes a comunicaciones electrónicas. El Verfassungsgerichtshof conoce de varios recursos en materia constitucional interpuestos por el Gobierno del Land de Carintia, los Sres. Seitlinger y Tschohl y otros 11.128 demandantes. En estos recursos se solicita la anulación de la disposición nacional que transpone la Directiva en el Derecho austriaco"[81].

El TJUE, en vista de las cuestiones planteadas, consideró que efectivamente los datos que se pueden obtener en virtud de la Directiva 2006/24/CE son muy sensibles. Con el conjunto de los datos que suponen las comunicaciones electrónicas de una persona se puede hacer un perfil muy preciso de la misma, en el que se incluyan hábitos, actividades, desplazamientos realizados ect..

El TJUE consideró que, "*al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes, la Directiva se inmiscuye de manera especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal*"[82].

Los motivos por los que el TJUE ha declarado inválida la Directiva 2006/24/CE son los siguientes[83]:

[81] Comunicado de prensa del TJUE de 8 de abril de 2014.
[82] Sentencia TJUE de 8 de abril de 2014.
[83] Comunicado prensa del TJUE de 8 de abril de 2014.

- La Directiva no hace excepciones con respecto a qué personas afecta, qué medios de comunicación electrónica comprende ni qué datos de tráfico se deben controlar en cada caso. El hecho de que no se establezca ninguna diferenciación, limitación o excepción, en función del objetivo de lucha contra los delitos graves, hace que la Directiva sea desproporcionada.

- En la directiva no se fijan criterios objetivos que permitan garantizar que las autoridades nacionales competentes únicamente tendrán acceso a los datos y podrán utilizarlos para prevenir, detectar o reprimir penalmente delitos que, por la magnitud y la gravedad de la injerencia en los derechos fundamentales en cuestión, puedan considerarse suficientemente graves para justificar tal injerencia.

- La Directiva se limita a remitir de manera genérica a los delitos graves definidos por cada Estado miembro en su ordenamiento jurídico interno. (En el caso de España dicha definición se encontraba recogida en el Código Penal y daba lugar a diversas interpretaciones). Además, "*la Directiva no define las condiciones materiales y procesales en las que las autoridades nacionales competentes pueden tener acceso a los datos y utilizarlos posteriormente*". No hay ningún órgano jurisdiccional u organismo administrativo autónomo que controle previamente el acceso a los datos.

- En cuanto al período de conservación de los datos, la Directiva establece un período mínimo de seis meses sin establecer ninguna distinción entre las categorías de datos en función de las personas afectadas o de la posible utilidad de los datos con respecto al objetivo perseguido. Además, este período varía entre seis meses como mínimo y veinticuatro meses como máximo, sin que "*la Directiva precise los criterios objetivos con arreglo a los que debe determinarse el período de conservación para garantizar que se limite a lo estrictamente necesario*".

- En la Directiva no se especifican garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y contra cualquier acceso y utilización ilícita de los datos. En particular, señala que "*la*

Directiva autoriza a los proveedores de servicios a tener en cuenta consideraciones económicas al determinar el nivel de seguridad que aplican".

- Por último, el TJUE hacer ver que la Directiva no obliga a que los datos se conserven en el territorio de la Unión. Por lo tanto, "*la Directiva no garantiza plenamente el control del cumplimiento de los requisitos de protección y de seguridad por una autoridad independiente*".

En vista de todos los razonamientos realizados en la STJUE de 8 de abril de 2014, el TJUE indica en su fallo que:

"La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, es inválida"[84].

III.4.3. Consecuencias STJUE de 18 de abril de 2014 y de la reforma de la LCrim

Como se ha indicado al principio de este apartado, la invalidez de la Directiva 2006/24/CE no conlleva automáticamente la invalidad de la Ley 25/2007, de 18 de octubre, de conservación de datos española.

El abogado especializado en nuevas tecnologías David Maeztu destaca en este sentido que:

"las modificaciones a la LCD están proyectadas desde antes de la sentencia del Tribunal de Justicia de la UE, mientras que hace hincapié en que en España el legislador no va a suspender la nomativa, ya que abriría la puerta a la anulación de los procedimientos penales en marcha. Es desde los juzgados desde donde se podría empezar a derribar la legislación"[85].

Uno de los mayores problemas que tenía la Ley 25/2007, de 18 de octubre, de conservación de datos española era el hecho de no definir lo que se entendía por

[84] Sentencia TJUE sobre los asuntos C-293/12 y C-594/12 de 8 de abril de 2014.
[85] EL DIARIO. 2014. Disponible en: http://www.eldiario.es/turing/vigilancia_y_privacidad/ley-conservacion-datos_0_259674834.html

delitos graves. Esta situación fue precisamente una de las pretendía evitar el TJUE con su Sentencia de 8 de abril de 2014.

La LO 13/2015, de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal, en su artículo 579, ha hecho una aproximación de lo que podría entenderse por delitos graves cubriendo así la ausencia de dicha definición en la Ley 25/2007, de 18 de octubre. Con la reforma de la LeCrim se entienden por delitos graves aquellos que tengan una pena límite máximo de al menos 3 años de prisión:

> ***"Once.*** *Se modifica el artículo 579, que quedará redactado del siguiente modo:*
>
> *Artículo 579 De la correspondencia escrita o telegráfica*
>
> ***1.*** *El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:*
>
> - ***1.º*** *Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.*
> - ***2.º*** *Delitos cometidos en el seno de un grupo u organización criminal.*
> - ***3.º*** *Delitos de terrorismo. (...)"*

Así mismo, la reforma de la LECrim ha introducido algunas novedades a mayores en la Ley 25/2007, de 18 de octubre:

(Artículos 588 ter j) LECrim)
La reforma acoge el criterio fijado por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, e impone la exigencia de autorización judicial para su cesión a los agentes facultados. Su incorporación al proceso solo se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones. Se da un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia.
Se regula el supuesto de la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo

electrónico, a los que podrá acceder el Ministerio Fiscal o la Policía Judicial en el ejercicio de sus funciones sin necesidad de autorización judicial[86].

La decisión del TJUE de invalidar la Directiva 2006/24/CE ha suscitado muchas reacciones en la doctrina, puesto que se trata de una decisión sin precedentes.

Ricard Martínez ha apuntado que:

"Por tanto, la Directiva vino a quebrar un modelo de tutela del secreto de las comunicaciones ampliando las capacidades de obtención de datos a toda la población y todo el tiempo, y pasando de una intervención reactiva a otra de naturaleza preventiva. Esto, que podría entenderse desde el punto de vista de los graves delitos potencialmente investigables no se limitó a la investigación de bandas terroristas o delincuencia organizada, se extendió a toda la población. Si sumamos las revelaciones de Snowden en el caso de la NSA, el contexto en el que se dicta la sentencia del TJUE en los asuntos C-293/12 y C-594/12, es cuando menos significativo"[87].

[86] LO 13/2015 de 5 de octubre de reforma de la LEcrim.
[87] MARTÍNEZ MARTÍNEZ R. 2014. Disponible en: http://lopdyseguridad.es/la-anulacion-de-la-directiva-200624ce/

IV. CONCLUSIONES

El derecho a la privacidad en Europa ha adquirido en los últimos años una gran importancia con el desarrollo de las nuevas tecnologías. En España, el derecho a la privacidad se ha configurado como un derecho fundamental a través del artículo 18.4 de la Constitución Española.

Existe una gran diferencia entre la concepción de la privacidad en los países con un modelo jurídico continental y en los países con un modelo jurídico anglosajón.

Mientras que en los países de tradición continental el derecho a la privacidad se configura como un derecho fundamental, en los países de tradición jurídica anglosajona éste se ha desarrollado a partir de resoluciones jurisprudenciales.

En países como Estados Unidos, difícilmente se comprende el exceso de celo por la privacidad que existe en la Unión Europea. Cuestiones como la seguridad ciudadana o derechos como el derecho a la información o el derecho a la libertad de expresión, chocan frontalmente con el derecho a la privacidad en más de una ocasión.

Las Sentencias dictadas por el TJUE en los últimos años no hacen otra cosa que confirmar la creciente preocupación por la preservación del derecho a la privacidad de los ciudadanos de la Unión Europea, así como fijar los límites a seguir en la aplicación del mismo.

La Sentencia más reciente de las analizadas en el presente trabajo, la STJUE dictada el pasado 6 de octubre de 2015 en relación con los acuerdos de Safe Harbor con Estados Unidos, es uno de los ejemplos más claros de la diferente forma de interpretar el derecho a la privacidad en ambos modelos jurídicos.

Sin embargo, la anulación de la decisión 2000/520/EC de la comisión europea por parte del TJUE (que ha supuesto la invalidación de los acuerdos de Safe Harbor) no debe interpretarse como una consecuencia de las revelaciones de Edward Snowden acerca de la intromisión de las agencias gubernamentales de Estados Unidos en los datos personales.

Sí es cierto que el caso Snowden ha influido en el fallo del TJUE, pero este último, en los fundamentos de la Sentencia dictada en el asunto C-362/14, ha analizado

aspectos que evidencian que la Comisión Europea ya no debería haber aceptado desde un primer momento los acuerdos de Safe Harbor.

La protección reconocida al tratamiento de los datos personales en los principios de puerto seguro nunca fue equiparable a la protección que se les da a los datos personales en la Directiva 95/46/CE. El mayor indicio con respecto a esta afirmación, lo encontramos en el hecho de que los acuerdos de Safe Harbor nunca han comprometido al gobierno de Estados Unidos a cumplirlos, sino solamente a las empresas que habían suscrito los mismos.

Podemos interpretar la Sentencia del TJUE de 6 de octubre de 2015 como una constatación de lo que ya muchas voces habían denunciado; que los acuerdos de Safe Harbor no dejaban de ser "papel mojado" que en realidad nunca han garantizado una efectiva protección de los datos personales transmitidos a Estados Unidos.

A la espera de confirmar si se podrá llevar a cabo un nuevo acuerdo de Safe Harbor que sí cumpla los requisitos establecidos por el TJUE, las empresas deben decidir qué medidas adoptar para evitar las cuantiosas sanciones que la LOPD prevé en el caso de las transmisión de datos internacionales sin la autorización del director de la AEPD.

Otra de las Sentencias analizadas fue la dictada por el TJUE el 13 de mayo de 2014 en el caso C-131/12, en relación con el reconocimiento del derecho al olvido.

Cabe destacar al hilo de esta Sentencia el importante papel que la AEPD ha desarrollado en el reconocimiento del derecho al olvido digital. Con varios años de anterioridad a la STJUE de 13 de mayo de 2014, la AEPD ya defendía la existencia de un derecho al olvido digital relacionado con los derechos de oposición y cancelación de los datos personales.

Es muy importante el análisis que hace el TJUE, en relación a que el derecho al olvido no puede implicar un atropello a los derechos de libertad de expresión e información cuando éste afecta a cuestiones de interés general. Debe realizarse siempre una correcta ponderación entre ambos derechos.

La solución aportada en el caso de los motores de búsqueda digitales, que consiste

que sean éstos los que realicen la ponderación entre el derecho al olvido y el derecho a la libertad de información y a la libertad de expresión, no es aceptable. No se puede permitir que una empresa privada (que se presupone que puede actuar de forma arbitraria) sea la que decida qué derecho fundamental debe primar a la hora de retirar o no un resultado de búsqueda relacionado con datos de carácter personal.

A pesar de la importancia que supone el reconocimiento del ejercicio del derecho al olvido directamente frente a los motores de búsqueda digitales, la cuestión realmente relevante de la STJUE dictada en el caso C-131/12 es la consideración de que la Directiva 95/46/CE debe de aplicarse a Google.

El hecho de que el establecimiento en España de Google esté directamente ligado a las actividades de promoción y publicidad de sus espacios publicitarios disponibles, hace que le sea de aplicación el concepto de establecimiento que recoge la Directiva 95/46/CE y la LOPD en su artículo 2.1.c). Para muchas empresas que no creían que les fuese de aplicación la Directiva 95/46/CE, la STJUE de 6 de octubre de 2015 ha supuesto que se tengan que adaptar a lo contemplado en la misma, y ello de forma inmediata sin un adecuado período de transición.

Por último, la Sentencia del TJUE de 8 de abril de 2014 resolviendo los casos C-293/12 y C-594/12, ha supuesto la invalidación de la Directiva 2006/24/CE de Conservación de Datos.

En España la transposición de la Directiva 2006/24/CE se ha realizado a través de la Ley 25/2007 de 18 de octubre de Conservación de Datos. El hecho de que la Directiva que ha originado la Ley 25/2007, de 18 de octubre haya sido invalidada no quiere decir que automáticamente sea invalidada dicha Ley.

La Sentencia del TJUE no deja de ser otro “tirón de orejas” a la actuación legislativa realizada a la hora de desarrollar la Directiva 2006/24/CE. La excesiva preocupación por la seguridad no puede anular el derecho a la privacidad de los ciudadanos.

Los límites que establecía la Directiva 2006/24/CE eran demasiado indefinidos y el hecho de que se guardasen indiscriminadamente los datos de todos los ciudadanos sin acotar los motivos por los que éstos se podrían solicitar a posteriori por los órganos facultados, era claramente una vulneración del derecho fundamental a la

intimidad.

De momento, en España, a pesar de las reformas introducidas en la LeCrim, no se han realizado cambios que supongan la adecuada adaptación de nuestra Ley 25/2007, de Conservación de Datos a lo dispuesto en la STJUE de 8 de abril de 2014.

Como conclusiones finales cabe reseñar que las Sentencias analizadas en este trabajo implican una clara tendencia por parte de la Unión Europea a reforzar y garantizar el derecho a la privacidad, pero también son la muestra de que el mismo no se estaba protegiendo de manera adecuada.

El hecho de que la mayoría de las compañías relacionadas con las nuevas tecnologías tengan su sede en países con un modelo jurídico anglosajón, ha supuesto que el tráfico de los datos personales se haya convertido en un gran negocio. A pesar de los esfuerzos de la Unión Europea por garantizar la protección del derecho a la privacidad y de los datos personales, éstos son cada vez más un objeto de comercialización y especulación a gran escala.

V. FUENTES JURÍDICAS UTILIZADAS

DOCTRINA Y ARTÍCULOS:

- ABANLEX. 2015. La Audiencia Nacional implementa en España la Sentencia del TJUE sobre derecho al olvido. [en línea] [consultado en 03/12/2015]. Acceso en: https://www.abanlex.com/2015/01/la-audiencia-nacional-implementa-en-espana-la-sentencia-del-tjue-sobre-derecho-al-olvido/

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2014. Derecho al olvido: 5 puntos clave para entender el derecho al olvido. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2014. Nota de prensa. El Tribunal de Justicia de la Unión Europea respalda los criterios de la AEPD en relación con los buscadores y el derecho al olvido en internet. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/may_14/NP_STJUE_derecho_olvido.pdf

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2014. Nota de prensa. Las autoridades europeas de protección de datos aprueban los criterios para aplicar la sentencia del “derecho al olvido”. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/nov_14/141128_NP_AEPD_Aplicacion_Sentencia_TJUE.pdf

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2015. Nota de prensa. El TJUE declara inválida la decisión de la comisión que declara el nivel adecuado de protección del Puerto Seguro. [en línea] [consultado en 01/12/2015]. Acceso en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_06-ides-idphp.php

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2015. Nota de prensa. Las autoridades europeas de protección de datos publican una declaración conjunta en relación con la aplicación de la sentencia del TJUE sobre el puerto seguro. [en línea] [consultado en 01/12/2015]. Acceso en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2015. Transferencias internacionales de datos. [en línea] [consultado en 03/12/2015]. Acceso en: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

- DANS, E. 2015. El “Safe Harbor” no era tan “Safe”. Artículo en línea para www.enriquedans.com [consultado en 03/12/2015]. Acceso en:http://www.enriquedans.com/2015/10/el-safe-harbor-no-era-tan-safe.html

- DERECHO AL OLVIDO. 2014. La bbc decide publicar su lista de enlaces eliminados por el derecho al olvido. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.derechoolvido.es/la-bbc-decide-publicar-su-lista-de-enlaces-eliminados-por-e

- DERECHO AL OLVIDO. 2015. Sentencia del tribunal supremo en un caso de derecho al olvido. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.derechoolvido.es/sentencia-del-tribunal-supremo-en-un-caso-de-derecho-al-olvido/

- ECIJA. 2015. Soluciones tras la invalidez del Safe Harbor. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.ecija.com/notas-de-prensa/nota-informativa-infografia-soluciones-tras-la-invalidez-de-safe-harbor/

- EL DIARIO.ES. 2014. El Gobierno dota de mayor eficacia a la Ley de Conservación de Datos. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.eldiario.es/turing/vigilancia_y_privacidad/ley-conservacion-datos_0_259674834.html

- EL DIARIO.ES. 2015. Sin noticias del Safe Harbor: sólo el 3% de las tecnológicas han hecho cambios. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.eldiario.es/hojaderouter/shortcut/Safe_Harbor-privacidad-proteccion_de_datos-empresas-terminos_y_condiciones_6_456064401.html

- EL MUNDO. 2015. Bruselas aprueba la nueva norma de Protección de Datos que reconoce el “derecho al olvido”. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.elmundo.es/tecnologia/2015/06/15/557e718646163f73038b456b.html

- EL PAÍS. 2015. Obama firma la Ley que impone límites al NSA. [en línea] [consultado en 03/12/2015]. Acceso en: http://internacional.elpais.com/internacional/2015/06/02/actualidad/1433277585_519201.html

- GALVAN BARCELÓ, J.C. 2015. LOPD, Safe Harbor: ¿Golpe de Timón del Derecho Anglosajón?. Artículo en línea para www.actualidadlopd.com [consultado en 03/12/2015]. Acceso en: http://www.actualidadlopd.com/2010/10/06/lopd-safe-harbor-%C2%BFgolpe-de-timon-del-derecho-anglosajon/

- HERNÁNDEZ RAMOS, M. 2013. El derecho al olvido digital en la Web 2.0. Cátedra Telefónica de la Universidad de Salamanca. (Cuadernos red de cátedras telefónica). [en línea]. (nº 11) [consultado en 03/12/2015]. ISSN: 2174-7628. Disponible en:

http://catedraseguridad.usal.es/sites/default/files/files/CUADERNO_11_DERECHO%20OLVIDO.pdf

- JIMÉNEZ DE LA IGLESIA, C. – ARMADA, C. R. 2015. Ante una nueva realidad. Artículo en línea para www.expansion.com [consultado en 03/12/2015]. Acceso en:http://www.expansion.com/juridico/opinion/2015/10/26/562e880346163fc4438b4593.html

- MARTÍNEZ MARTÍNEZ, R. 2014. La anulación de la directiva 2006/24/CE. Artículo en línea para www.lopdyseguridad.es [consultado en 03/12/2015]. Acceso en: http://lopdyseguridad.es/la-anulacion-de-la-directiva-200624ce/

- MARTÍNEZ MARTÍNEZ, R. 2015. Safe Harbour y la privacidad en Europa. Artículo en línea para www.bez.es [consultado en 03/12/2015]. Acceso en:http://www.bez.es/578211217/Safe-Harbour-y-el-modelo-europeo-de-proteccion-de-datos..html#posicion_2

- MURILLO DE LA CUEVA, P.L. 2007. Perspectivas del derecho a la autodeterminación informativa. Revista Internet, Dret i Política. [en línea]. (nº 5) págs. 18-32 [consultado en 03/12/2015]. ISSN: 1699-8154. Disponible en:http://www.uoc.edu/idp/5/dt/esp/lucas.pdf

- NOTICIAS JURÍDICAS. 2015. Primera sentencia del TS sobre el derecho al olvido: si los interesados lo solicitan la información obsoleta sobre personas sin relevancia pública puede no ser buscable. [en línea] [consultado en 03/12/2015]. Acceso en: http://noticias.juridicas.com/actualidad/noticias/10588-primera-sentencia-del-ts-sobre-el-derecho-al-olvido:-si-los-interesados-lo-solicitan-la-informacion-obsoleta-sobre-personas-sin-relevancia-publica-puede-no-ser-buscable/

- ROIG BATALLA, A. 2011. Derechos fundamentales y tecnologías de la información y de las comunicaciones (Tics). España: J.M. BOSCH EDITOR. [consultado en 19/09/2015]. Acceso en: ProQuest ebrary.

- SALGADO SEGUÍN, V.A. 2010. Intimidad, privacidad y honor en Internet. Revista TELOS (Cuadernos de Comunicación e Innovación) [en línea]. (nº 85) págs. 69-79 [consultado en 19/09/2015]. ISSN: 0213-084X. Disponible en:https://telos.fundaciontelefonica.com/seccion=1268&idioma=es_ES&id=20101010409480001&activo=6.do

- SERJUTECA. 2015. Las 10 claves de la modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. (Ley Orgánica 13/2015, de 5 de octubre. BOE de 6 de octubre). [En línea] [Consultado en 03/12/2015]. Acceso en: http://www.serjuteca.es/static/pdf/LECR_CLAVES_DE_LA_REFORMA_web.pdf

- SIMÓN CASTELLANO P. 2015. El reconocimiento del derecho al olvido digital en España y en la UE. 1ª edición, Barcelona, Bosch, págs. 166, 180-181, 197,

204-221, 294-296, 300-301 y 306-307.

- TICBEAT. 2015. EEUU y la UE alcanzan un acuerdo para actualizar el safe harbor. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.ticbeat.com/tecnologias/eeuu-la-ue-alcanzan-acuerdo-para-actualizar-el-safe-harbor/

- URÍA MENÉNDEZ ACTUALIDAD JURÍDICA. 2014. Sentencia Google Spain y Derecho al olvido. [en línea] [consultado en 03/12/2015]. Acceso en: http://www.uria.com/documentos/publicaciones/4370/documento/fe04.pdf?id=5584

LEGISLACIÓN:

- Asamblea General Naciones Unidas. Declaración Universal de los Derechos Humanos. 10 de diciembre de 1948.
    - Artículo 12.

- España. Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311.
    - Artículo 10.1.
    - Artículo 18.

- España. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Boletín Oficial del Estado, 19 de octubre de 2007, núm. 251.
    - Artículo 1.

- España. Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Boletín Oficial del Estado, 31 de octubre de 1992, núm. 262.
    - Exposición de motivos.

- España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 14 de diciembre de 1999, núm. 298.
    - Artículo 2.
    - Artículo 3.
    - Artículo 5.
    - Artículo 11.1.
    - Artículo 33.
    - Artículo 34.

- Artículo 44.4.
- Artículo 45.3

- España Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Boletín Oficial del Estado, 6 de octubre de 2015, núm. 239.

  - Artículo 11.

- España. 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. Boletín Oficial del Estado, 19 de enero de 2008, núm. 17.

  - Artículo 68.

- Roma. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. 4 de noviembre de 1950.

  - Artículo 8.

- Unión Europea. Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Diario Oficial de la Unión Europea, 15 de marzo de 2006.

  - Considerando 1.

- Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, 24 de octubre de 1995.

RESOLUCIONES:

1984

- España. Tribunal Constitucional (Sala Primera) [Internet]. Sentencia 110/1984, de 26 de noviembre de 1984. [consultado 4 diciembre 2015]. Disponible en: http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/363

1993

- España. Tribunal Constitucional (Sala Primera) [Internet]. Sentencia

254/1993, de 20 de julio de 1993. [consultado 4 diciembre 2015]. Disponible en: http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/2383

2000

- España. Tribunal Constitucional (Pleno) [Internet]. Sentencia 292/2000, de 30 de noviembre de 2000 [consultado 4 diciembre 2015]. Disponible en: http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4276

2009

- España. Agencia Española de Protección de Datos. Resolución núm. D/00771/2009 AEPD

2013

- Tribunal de Justicia de la Unión Europea. Caso Google Spain S.A., Google Inc, contra Agencia Española de Protección de Datos, Mario Costeja López (C-131/12). [Internet]. Conclusiones del abogado general de 25 junio 2013. [consultado 4 diciembre 2015]. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES

2014

- España. Audiencia Nacional (Sala de lo Contencioso Administrativo) [Internet]. Sentencia 5129/2014, de 29 de diciembre de 2014 [consultado 4 diciembre 2015]. Disponible en: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-establece-los-criterios-para-reconocer-el--derecho-al-olvido-

- Tribunal de Justicia de la Unión Europea. Caso Google Spain S.A., Google Inc, contra Agencia Española de Protección de Datos, Mario Costeja López (C-131/12). [Internet]. Sentencia de 13 de mayo de 2014. [consultado 4 diciembre 2015]. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

- Tribunal de Justicia de la Unión Europea. Caso Digital Rights Ireland y Seitlinger y otros. (C-293/12 y C-594/12) [Internet]. Sentencia de 8 de abril de 2014. [consultado 4 diciembre 2015]. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=ES

- Tribunal de Justicia de la Unión Europea. Caso Digital Rights Ireland y Seitlinger y otros. (C-293/12 y C594/12) [Internet]. Comunicado de prensa 54/14 de 8 de abril de 2014. [consultado 4 diciembre 2015]. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-

04/cp140054es.pdf

2015

- España. Tribunal Supremo (Sala de lo Civil) [Internet]. Sentencia 545/2015, de 15 de octubre de 2015 [consultado 4 diciembre 2015]. Disponible en: http://www.poderjudicial.es/cgpj/es/Temas/Documentacion-Judicial/Jurisprudencia-/Sentencias-de-actualidad/Tribunal-Supremo/TS-Civil--Estima-en-parte-el-recurso-de-casacion-interpuesto-por--Ediciones-El-Pais-SL---Derecho-al-olvido-digital--Revoca-los-pronunciamientos-relativos-a-la-supresion-de-los-datos-personales-en-el-codigo-fuente-y-del-nombre--apellidos-o-incluso-iniciales--y-a-la-prohibicion-de-indexar-los-datos-personales-para-su-uso-por-el-motor-de-busqueda-interno-de-la-hemeroteca-digital-

- Tribunal de Justicia de la Unión Europea. Caso Maximillian Schrems y Data Protection Commissioner. (C-362/14) [Internet]. Sentencia de 6 de octubre de 2015. [consultado 4 diciembre 2015]. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

- Tribunal de Justicia de la Unión Europea. Caso Maximillian Schrems y Data Protection Commissioner. (C-362/14) [Internet]. Comunicado de prensa 117/15 de 6 de octubre de 2015. [consultado 4 diciembre 2015]. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf