Universidad de Valladolid

icava
Ilustre Colegio de Abogados de Valladolid

TFM Máster de Acceso a la Abogacía Curso 2018/2020

"Ley aplicable y autoridad competente en materia de protección de datos. El caso *Weltimmo*"

Presentado por:

Doña Sandra Pérez Bastardo

Tutelado por:

Don Dámaso Francisco J. Vicente Blanco

En Valladolid, febrero de 2020.

ÍNDICE

1. SUPUESTO DE HECHO

Asunto C-230/14, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Kúria [Tribunal Supremo] (Hungría), mediante resolución de 22 de abril de 2014, recibida en el Tribunal de Justicia el 12 de mayo de 2014, en el procedimiento entre:

Weltimmo s.r.o. y **Nemzeti Adatvédelmi és Információszabadság Hatóság**.

1.1. Litigio Principal

1º Los hechos se desarrollaron en una sociedad constituida en Eslovaquia (**Weltimmo**), la cual gestiona un sitio de Internet, de anuncios de inmuebles situados en Hungría.

2º *Weltimmo* en el contexto anteriormente referenciado, trata los datos de carácter personal de los anunciantes. Los anuncios son gratuitos durante un mes, transcurrido dicho plazo, el servicio pasa a ser de pago. Numerosos anunciantes solicitaron, vía correo electrónico, la retirada de sus anuncios a partir de dicho plazo, así como la supresión de sus datos de carácter personal.

3º Al contrario de lo que solicitan los interesados *Weltimmo* hizo caso omiso a la solicitud de supresión de los datos de carácter personal de los anunciantes, además facturó sus servicios a los interesados. Ante el impago de esas facturas, *Weltimmo* trasmitió los datos de carácter personal de los anunciantes a una serie de empresas de cobro de impagos.

4º Ante los hechos anteriormente expuestos, los anunciantes presentaron una serie de denuncias ante la autoridad de control húngara. Dicha autoridad se declaró competente, dado que estimaba que la recogida de datos sobre la que versa el asunto se había realizado en territorio húngaro y que constituía un tratamiento de datos de carácter personal relativo a personas físicas. Dicha autoridad interpuso a Weltimmo una multa de unos 32.000€.

5º Cuando *Weltimmo* conoció la sanción que se le había impuesto acudió al Tribunal Contencioso-Administrativo de Budapest. Dicho Tribunal consideró que el hecho de que la sociedad no dispusiese de domicilio social o establecimiento permanente en Hungría no era suficiente para la defensa, dado que el tratamiento de datos de carácter personal

de los anunciantes se había realizado en Hungría.

6º *Weltimmo* recurrió en casación ante el órgano jurisdiccional remitente, alegando que en base al **artículo 28.6 de la Directiva 95/46**, la autoridad de control húngara debió haber instado a la autoridad eslovaca competente en la materia, para que actuase en su lugar y no haberse declarado competente.

7ª A lo descrito en el anterior punto, la autoridad de control húngara alegó que la sociedad en cuestión contaba con un representante en Hungría, el cual era de nacionalidad húngara y que además era uno de los propietarios de la sociedad Weltimmo. Añadiendo que, aunque los servidores de la sociedad no se encuentran en Hungría sí que lo hacen residiendo sus propietarios. Por lo cual en virtud del **artículo 28.6 de la Directiva 95/46** se establece su competencia, independientemente del derecho que le sea aplicable al caso concreto.

8º Finalmente, dado que la Kúria contaba con una serie de dudas en relación a la determinación del Derecho aplicable y las facultades de la autoridad de control húngara decidió suspender el procedimiento y plantear al Tribunal de Justicia de la Unión Europea una serie de cuestiones prejudiciales.

1.2. Cuestiones Prejudiciales

El Tribunal Supremo (**TS**) de Hungría, en aras de un mejor análisis, plantea al Tribunal de Justicia de la Unión Europea (**TJUE**) ocho preguntas, las cuales el **TJUE** divide en tres bloques para un mejor análisis.

BLOQUE I (Cuestión prejudicial de 1 a 6)

El bloque I trata de esclarecer si la autoridad de control de un Estado Miembro (de Hungría en el caso concreto) se encuentra legitimada para poder aplicar su legislación nacional (ley aplicable) al responsable del tratamiento de datos (empresa), el cual lleva a cabo una actividad a través de internet, a pesar de estar registrado en otro Estado miembro distinto de donde presta sus servicios.
Para determinar lo anterior, el TJUE utiliza como medio el siguiente articulado:

- **Artículo 4.1.a) Directiva 95/46**, versa sobre el derecho nacional aplicable.
- **Artículos 28.1, 3 y 6 de la Directiva 95/46**, los cuales tratan sobre las funciones y facultades de las autoridades de control de datos.

Para empezar el **TJUE** realiza la interpretación del **art. 4.1.a) de la Directiva**, a lo cual indica que, si el responsable del tratamiento realiza una ***actividad real y efectiva,*** *aunque sea mínima a través de una* ***instalación estable*** en el territorio del Estado miembro del que la autoridad de control es dependiente, ésta (en este caso Hungría) se encontrara legitimada para aplicar su legislación nacional.

No obstante, el **TJUE** indica en su ST que es tarea del tribunal nacional y no suya el determinar si lo indicado anteriormente ocurre, dando una serie de pautas para poder hacerlo.

Antes que nada, el **TJUE** deja claro que carece de relevancia para el caso y por lo tanto para los siguientes casos que ocurran similares a "***Weltimmo"*** el hecho de que los anunciantes en la página web sean de nacionalidad húngara.

Para llegar a la interpretación del ***art. 4.1.a) de la Directiva*** anteriormente indicada el TJUE realiza dos interpretaciones, para las cuales utiliza de forma análoga a la Sentencia el caso ***"Google Spain"***:

- Concepto de **"Establecimiento"**

Para determinar dicho concepto el **TJUE** toma como guía los ***considerandos 18 y 19 de la Directiva 95/46***, en los cuales se establece un ámbito de aplicación territorial muy amplio, por lo cual el Tribunal y además estando totalmente en consonancia con lo indicado por el Abogado General en su informe considera que ha de preponderar **"*una concepción flexible de la noción de establecimiento",*** de tal manera que como ocurre en este caso con un único representante podrá ser suficiente para considerarse que la empresa cuenta con un establecimiento estable en el Estado en discordia.

En base por tanto a lo indicado, el Tribunal concluye que ***"Weltimmo"*** ejerce una actividad real y efectiva en el territorio de Hungría.

- Determinar si el tratamiento de datos se produjo **"en el marco de las actividades de dicho establecimiento"**

Para dilucidar si el tratamiento de datos de carácter personal se llevó a cabo en el marco de las actividades del establecimiento en este caso en Hungría, se basa como ya hemos indicado antes en la *ST Google Spain*, de tal manera que indica que en la referencia a datos personales en una página de Internet se incluye en la noción de "tratamiento" en el sentido del **artículo 2 de la Directiva 95/46**, y tampoco cabe duda que , en el caso Weltimmo dicho tratamiento se efectúa en el marco de la gestión de las páginas web a través de las que se anuncian los inmuebles situados en Hungría.

Por lo cual, se considera que **el artículo 4.1.a)** posibilita la aplicación del derecho nacional de Hungría en una situación como la del caso *"Weltimmo".*

BLOQUE II (Cuestión prejudicial 7)

El Bloque II se centra en establecer la legitimación o no de la autoridad de control de un Estado Miembro para imponer una sanción pecuniaria al responsable del tratamiento a pesar de que se hubiese determinado con anterioridad que la legislación aplicable al tratamiento de datos no fuese la de ese Estado miembro.

Para dilucidar dicha legitimación el **TJUE** toma como medio el **artículo 28 de la Directiva 95/46** en varios de sus puntos:

En primer lugar, se determina que la interpretación del presente artículo ha de realizarse de tal manera que la autoridad de control debe de limitar sus funciones al territorio de su Estado Miembro, las funciones vienen determinadas por el punto 3 del artículo 28, el cual indica textualmente:

"La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;

- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del

tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;

- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial."

Dicha lista, no es una lista cerrada, dado que más adelante en la propia Directiva podemos encontrar como se le da potestad de sancionadora a dicha autoridad.

Por consiguiente y en virtud de del principio de soberanía territorial, del principio de legalidad y del concepto de Estado de Derecho, la potestad sancionadora de dicha autoridad no puede extenderse más allá de su territorio nacional.

Para concluir, se desprende de la ***ST Weltimmo*** como hemos indicado en el párrafo anterior que la autoridad de control de un estado miembro no puede extender su potestad sancionadora fuera de su territorio, pero además ***"deberá instar la intervención de la autoridad de control dependiente del Estado miembro cuyo Derecho es aplicable".***

BLOQUE III (Cuestión prejudicial 8)

El bloque III, el cual es el más breve de los tres, se encarga de responder a la siguiente cuestión:

"En la terminología de la Directiva de protección de datos, ¿puede considerarse que el concepto de "adatfeldolgozás" empleado tanto en el artículo 4, apartado 1, letra a), como en el artículo 28, apartado 6, de la [versión húngara de la] Directiva, ¿es idéntico al concepto de "adatkezelés")

Para dar respuesta a lo anteriormente indicado el TJUE utiliza la propia Directiva, determinando finalmente que el concepto de «adatfeldolgozás» empleado en los artículos 4, apartado 1, letra a), y 28, apartado 6, de la versión húngara de la Directiva 95/46, ha de ser interpretado en el sentido de que incluye tanto el tratamiento de datos en sentido amplio, como la ejecución de tareas técnicas realizadas en relación con las operaciones de tratamiento de datos.

2. PRESENTACIÓN Y OBJETO DEL DICTÁMEN

En base a lo descrito anteriormente y ante la solicitud de resolución de las cuestiones prejudiciales planteadas por la Kúria **se puede comprobar cómo** el caso muestra con claridad los límites del juego de los principios de territorialidad y personalidad de las leyes, así como los límites de territorialidad de las competencias de la autoridad. Por lo indicado el dictamen jurídico versara sobre las siguientes cuestiones:

1.- ¿Qué vínculos territoriales considera relevantes el tribunal y con que alcance?

a) El lugar del establecimiento del gestor de los datos

b) El lugar de gestión o de transmisión de los datos

c) El lugar de localización del servidor

d) El lugar de situación de los inmuebles de las transacciones

e) El lugar de residencia de los propietarios de los bienes

2.- ¿Qué relevancia tendría el criterio de la nacionalidad en el caso a la luz de la decisión del TJUE?

3.- ¿Hasta dónde alcanza el límite de la competencia de autoridad en el caso? ¿Le parece razonable?

El objetivo principal del presente dictamen es dilucidar los distintos ámbitos y cuestiones que surgen a lo largo de la se STJUE de 1 octubre 2015, C-230/14, "*Weltimmo*", sobre todo centrándonos en la ley aplicable y la autoridad competente en materia de protección de datos, utilizando las cuestiones prejudiciales como principal fuente de análisis.

3. MATERIAL DE TRABAJO UTILIZADO

En primer lugar, antes de comenzar a exponer el material de trabajo utilizado para elaborar el presente dictamen, esta parte considera necesario hacer una breve aclaración:

Como bien sabemos la Sentencia en la que se basa el presente Trabajo data de fecha 1 de octubre del 2015, por lo cual, la normativa aplicable en el momento de la resolución de dicha sentencia no es la misma que se utilizaría si esto ocurriese a fecha actual (año 2020). En base a esto, en primer lugar, se analizará la normativa que se aplicó en el año 2015 y posteriormente se realizará un breve análisis de la normativa que aplicaría al mismo caso si la controversia se diese en la actualidad.

3.1. NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS AÑO 2015

3.1.1. En el marco de la Unión Europea (UE)

a) Directiva 95/46 del Parlamento Europeo y del Consejo

En la Unión Europea se adoptó la **Directiva 95/46** del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo respectivo al tratamiento de datos de carácter personal y a la libre circulación de estos. Dicha Directiva adoptada en 1995 se basaba en regular el procesamiento de datos de carácter personal, independientemente de si tal procesamiento era automatizado o no, en el espacio de la Unión Europea.

De la presente Directiva, cabe destacar el espíritu conciliador con el que cuenta, dado que intenta compaginar el tratamiento de los datos de carácter personal con la tutela de los derechos de las personas físicas. Tal y como podemos encontrar en el artículo 1 de la Directiva 95/46, los Estados miembros deberán garantizar:

"la protección de las libertades y los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos de carácter personal".

A mayor abundamiento, la Directiva 95/46 cuenta con tres principios como pilares básicos, que son:

Principio de Transparencia: El interesado tiene derecho a ser informado de cómo van a ser tratados sus datos.

Principio de Legitimidad: ***"Los datos personales solamente pueden ser recogidos para finalidades determinadas, explícitas y legítimas, y no pueden ser tratados posteriormente de manera incompatible con estas finalidades"*** (Art. 6 b Directiva 95/46).

Principio de Proporcionalidad: Los datos de carácter personal que van a ser tratados han de ser los adecuados, pertinentes y no excesivos en relación a la finalidad para la cual fueron recogidos.

Finalmente, respecto de la presente Directiva, esta parte considera necesario hacer referencia al ámbito de aplicación, el cual se basa en dos puntos:

- Que se trate de un dato de carácter personal, relativo a una persona física.
- Que mediante dicho dato personal se refiera a una persona identificada o identificable. (*Por ejemplo:* no entraría dentro del ámbito de aplicación de la directiva la realización de una encuesta de forma anónima)

En lo que respecta a la concreción de la ley aplicable, también se determina en la Directiva el Estado o Estados Miembros cuyas autoridades eran competentes en lo que respecta a la supervisión, esto es así debido a la relación tan estricta que existe entre ***ley aplicable y autoridad competente.*** Todo lo indicado se pone de relieve en la ST Weltimmo, sobre la que versa el presente TFM.

Finalmente, indicar que la Directiva fue derogaba el 25 de mayo de 2018, por el inicio de la plena aplicación del **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo**, de 27 de abril de 2016, el cual analizaremos en detalle más adelante.

b) El Grupo de Trabajo del Artículo 29 (GT29)

Dicho Órgano se encuentra compuesto por un representante de la autoridad de protección de datos de cada estado miembro de la Unión Europea (**UE**), el Supervisor Europeo de Protección de Datos y la Comisión Europea. Se trata de un órgano de carácter consultivo y con independencia de la UE. Su nombre proviene de la **Directiva 95/46 CE** y fue lanzado en el año 1996 para poder llevar a cabo una evaluación de la implementación de las empresas de la normativa en materia de protección de datos.

Entre sus funciones cabe destacar las siguientes:

Su principal función no es otra que, facilitar a la Comisión Europea dictámenes sobre las leyes comunitarias que tengan cabida en la protección de datos.
Dar consejos de expertos a los Estados en lo que tiene que ver con la normativa en materia de protección de datos vigente en el momento (**Directiva 95/46**).
Promover la correcta aplicación de la **Directiva 95/46** en los Estados que forman parte de la UE. Así como en Noruega, Liechtenstein e Islandia (en virtud del acuerdo EEE).

Dentro de los Dictámenes que tiene como función emitir, encuentra esta parte interesantes en relación con la Sentencia sobre la que versa el presente TFM los siguientes:
Dictamen 8/2010 sobre ley aplicable, en éste se abordan las principales controversias y cuestiones sobre el derecho aplicable, en concreto, los *artículos 4, 17 y 28 de la Directiva 95/46*. Dichos artículos se centran en definir tanto el derecho aplicable, como la autoridad que ha de encargarse de la aplicación del determinado derecho. En el dictamen se le da una gran importancia a la estrecha relación que existe entre derecho material y jurisdicción.
Como conclusiones importantes cabe citar textualmente las del dictamen:
"La disposición clave sobre el Derecho aplicable es el artículo 4, que determina qué disposición(disposiciones) nacional(es) de protección de datos aprobada(s) para la aplicación de la Directiva puede(n) aplicarse al tratamiento de datos personales.
De conformidad con el artículo 4, apartado 1, letra a), un Estado miembro aplicará su Derecho nacional de protección de datos cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Para la determinación de un establecimiento relevante para los efectos del artículo 4, apartado1, letra a), es clave que el organismo en cuestión realice un ejercicio efectivo y real de actividades. Además, la referencia a "un" establecimiento significa que la aplicabilidad del Derecho de un Estado miembro se desencadenará por la ubicación de un establecimiento del responsable del tratamiento en ese Estado miembro y los Derechos de otros Estados miembros podrían desencadenarse por la ubicación de otros establecimientos de ese responsable del tratamiento en esos Estados miembros.
La noción de "marco de actividades" –y no la ubicación de los datos– es un factor determinante en la determinación del ámbito del Derecho aplicable. La noción de "marco de actividades" implica que el Derecho aplicable no es el del Estado

miembro en el que esté establecido el responsable del tratamiento, sino en el que un establecimiento del responsable del tratamiento esté implicado en actividades relativas al tratamiento de datos personales. En este contexto, es crucial el grado de implicación del (de los) establecimiento(s) en las actividades en cuyo marco se traten los datos personales.

Además, debe considerarse la naturaleza de las actividades de los establecimientos y la necesidad de garantizar una protección efectiva de los derechos de las personas. En el análisis de estos criterios debe adoptarse un enfoque funcional: más que la indicación teórica por las partes del Derecho aplicable, lo que debería ser decisivo son su comportamiento e interacción en la práctica.

El artículo 4, apartado 1, letra b), aborda el caso menos común en que el Derecho de protección de datos del Estado miembro se aplica cuando "el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público". Criterios externos (34) *derivados del Derecho internacional público determinarán en situaciones específicas la extensión de la aplicación del Derecho nacional de protección de datos fuera de las fronteras nacionales, por ejemplo, en el caso de embajadas o buques.*

El artículo 4, apartado 1, letra c), procura garantizar el derecho a la protección de datos personales contemplado por la Directiva aun cuando el responsable del tratamiento no esté establecido en el territorio de la UE/del EEE, pero el tratamiento tenga alguna conexión con dicho territorio. Para garantizar la coherencia dentro del artículo 4 y para evitar lagunas en la aplicación del Derecho de protección de datos, el Grupo considera que la existencia de un establecimiento del responsable del tratamiento en territorio comunitario no debería impedir la aplicación del artículo 4, apartado 1, letra c), cuando dicho establecimiento no sea un establecimiento relevante a los efectos del artículo 4, apartado 1, letra a). En cambio, debería aplicarse la disposición "recurrir a medios" del artículo 4, apartado1, letra c), en aquellos casos en que no haya ningún establecimiento en la UE/el EEE que desencadene la aplicación del artículo 4, apartado 1, letra a) o en que el tratamiento no se sea efectuado en el marco de dicho establecimiento.

El elemento crucial que determina la aplicabilidad del artículo 4, apartado 1, letra c), y, en consecuencia, la del Derecho de protección de datos de un Estado miembro, es el recurso a medios situados en el territorio de dicho Estado miembro.

El concepto de "recurrir a medios" presupone dos elementos: algún tipo de actividad del responsable del tratamiento y la clara intención del mismo de tratar datos personales. Por consiguiente, aunque no cualquier utilización de medios dentro del territorio de la UE/del EEE conduce a la aplicación de la Directiva, no es necesario que el responsable del tratamiento tenga la propiedad o pleno control de tales medios para que el tratamiento caiga dentro del ámbito de la Directiva.

Respecto a la noción de "equipment" (equipo) en la versión inglesa, su expresión como "medios" en otras lenguas de la UE llevaría a una amplia interpretación de los criterios, que favorecería un amplio ámbito de aplicación. Esta interpretación puede, en algunos casos, tener como resultado que el Derecho europeo de protección de datos sea aplicable cuando el tratamiento en cuestión no tenga una conexión real con la UE/EEE. En cualquier caso, el tratamiento de datos personales por un responsable del tratamiento establecido fuera de la UE/del EEE, a través de medios situados en la UE/el EEE, desencadena la aplicación de la Directiva de conformidad con el artículo 4, apartado 1, letra c), lo que significa que todas las restantes disposiciones relevantes de la Directiva serán también aplicables.

Se excluye la aplicación del Derecho nacional de un Estado miembro cuando los medios utilizados por el responsable del tratamiento y situados en el Estado miembro se utilizan solo para garantizar el tránsito por el territorio de la Unión, por ejemplo, en el caso de redes de telecomunicaciones (cables) o servicios postales que solo garantizan que las comunicaciones transiten por el territorio de la Unión hasta alcanzar los terceros países.

El artículo 4, apartado 2, impone al responsable del tratamiento la obligación de designar un "representante" en el territorio del Estado miembro cuyo Derecho sea aplicable en virtud de la utilización por dicho responsable del tratamiento de medios situados en ese Estado miembro para tratar datos personales. En este último caso, la ejecución contra un representante puede ser muy difícil.

El artículo 17, apartado 3, establece que el contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento deberá asimismo estipular que el encargado del tratamiento debe cumplir las medidas de seguridad "tal como las define la legislación del Estado miembro en el que esté establecido el encargado". La razón que está detrás de este principio es garantizar requisitos uniformes dentro de un Estado miembro en relación con las medidas de seguridad,

así como facilitar su ejecución.

El objetivo del artículo 28, apartado 6, es colmar la diferencia entre el Derecho aplicable y la jurisdicción de control que pudiera surgir en el campo de protección de los datos dentro del mercado interior, estableciendo que la autoridad de protección de los datos debe poder ejercer sus poderes de verificación e intervención en una operación de tratamiento que tenga lugar en su territorio aun cuando el Derecho aplicable sea el de otro Estado miembro." [1]

El **GT29** no solamente se queda aquí, sino que al final de su dictamen realiza una serie de recomendaciones en aras de mejorar las disposiciones vigentes al respecto, dado que a la hora de elaborar el presente dictamen ha detectado una serie de deficiencias, sobre todo en la parte que tiene que ver con el derecho aplicable (*Art. 4 Directiva 45/96*), esto es así, ya que se considera por el **GT29** que los términos utilizados no son los óptimos, sino que son necesarios de aclaración ulterior.

Actualización Dictamen 8/2010, sobre ley aplicable: En aras de adecuar a las nuevas situaciones, debido al paso del tiempo, en el año 2016 el GT29 considero necesario llevar a cabo una actualización del Dictamen. Unos de los principales motivos para llevar a cabo esta actualización es el alto impacto que tuvo la determinación de la ley aplicable tanto en la Sentencia sobre la que versa el presente TFM (**ST TJUE** *"Weltimmo"*), como en la conocidísima **ST TJUE** *"Google Spain"*, dado que las implicaciones de ambas Sentencias van más allá de la simple determinación de la ley aplicable, por lo cual incorpora en su dictamen el análisis en profundidad de los siguientes términos:

"En el marco de las actividades de un establecimiento"

"Vínculo indisociable"

Se incorporan por tanto los citados cambios en el Dictamen 8/2010, así como se aprovecha para añadir una serie de ejemplos que puedan ayudar en los casos futuros en los que haya casos similares en los que sea necesario determinar la ley aplicable.

El GT29 se ha visto sustituido por el **Comité Europeo de Protección de Datos,** lo cual se ha producido debido a la entrada en vigor del Reglamento Europeo de Protección de datos (**RGPD**). Ambos serán analizados en detalle más adelante.

[1] Dictamen 8/2010 sobre ley aplicable Grupo de Trabado del artículo 29. < http://www.informatica-juridica.com/anexos/dictamen-8-2010-del-16-de-diciembre-de-2010-sobre-el-derecho-aplicable-emitido-por-el-grupo-de-proteccion-de-datos-del-articulo-29-nbsp-wp-179/>

3.1.2. Normativa en España

a) Ley Orgánica, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD 15/1999)

Su principal objeto fue tal y como se indicaba textualmente en su **artículo 1:**

"el de garantizar y proteger, en lo que concierne al tratamiento de datos de carácter personal., las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar" [2]

Si bien es cierto, la **LOPD 15/1999** debió de ser desarrollado por el **Real Decreto 1720/2007**, de 21 de diciembre, el cual desarrolla tanto los principios de la ley, como las medidas de seguridad a aplicar en los sistemas de información.

Será de aplicación la presente Ley Orgánica en los siguientes casos:

El tratamiento de datos de carácter personal sea realizado en territorio español, en el marco de las actividades de un establecimiento del responsable del tratamiento.

En el caso de que el responsable del tratamiento no esté establecido en territorio español, pero le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

Si el responsable del tratamiento no se encuentra dentro de la UE, pero para realizar dicho tratamiento utilice medios situados en el territorio español (con la salvedad de que sea con fines de transito).

Por otra parte, en lo que respecta al órgano público de control de cumplimiento de dicha normativa con carácter general en España es la Agencia Española de Protección de Datos (AEPD), la cual como ya hemos indicado se encarga de velar por el cumplimiento de la normativa española en materia de protección de datos.

Finalmente, cabe añadir que la **LOPD 15/199** fue derogada con la entrada en vigor, el 6 de diciembre de 2018, de la **Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales**, que adapta la legislación española al Reglamento General de Protección de Datos de la Unión Europea. Dicha normativa actual será tratada

[2] LOPD 15/99 < https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf>

en detalle en el siguiente apartado.[3]

3.2. NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS EN LA ACTUALIDAD

3.2.1. En el marco de la Unión Europea (UE)

a) Reglamento General de Protección de Datos (RGPD)

Tras más de un lustro de gestación, en la actualidad contamos con el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,* relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y *por el que se deroga la Directiva 95/46/CE* se aprobó el 14 de abril 2016, pero no fue de plena aplicación hasta el 25 de mayo de 2018 con el fin de unificar en todos los estados miembros sobre la materia de protección de datos.

Respecto del ámbito de aplicación territorial, dispuesto en su propio *art. 3 RGPD, nos indica que el Reglamento será de aplicación cuando:*

"El tratamiento de datos personales se realice en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

Cuando el responsable o encargado no estén establecidos en la Unión, el RGPD resultará aplicable al tratamiento de datos personales de interesados que residan en la Unión si las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios en la Unión a dichos interesados, independientemente de si a estos se les requiere su pago, o con el control de su comportamiento, en la medida en que este tenga lugar en la Unión." [4]

Conviene señalar en este punto algunas de las principales diferencias y novedades del RGPD respecto de la normativa anterior (LOPD 15/1999) en lo que tiene que ver con la incorporación de una serie de nuevos principios:

Protección de Datos por defecto y desde el diseño: Se indica la importancia de adoptar medidas que garanticen el cumplimiento de la norma desde el mismo momento en que se

[3] **MEMENTO PRÁCTICO SOBRE PROTECCIÓN DE DATOS (2019-2020).** Lefebvre.

[4] **Reglamento General de Protección de Datos** < https://www.boe.es/doue/2016/119/L00001-00088.pdf>

diseñe una empresa, producto, servicio o actividad que implique tratamiento de datos de carácter personal. Es decir, no esperar para implementar la normativa de protección de datos, sino realizarla desde los inicios.

Principio de Responsabilidad Proactiva o "Accountability": Las entidades han de poder probar que están cumpliendo con las premisas que indica la norma. Es decir, no basta solo con cumplir la normativa, sino que tienen que estar en aras de poder demostrarlo mediante procedimientos internos, etc.

Principio de Transparencia: Los textos legales que tienen que ver con la normativa en materia de protección de datos **deberán de ser** más simples e inteligibles, facilitando su comprensión, además de más completos. Esto es así debido a que prima la facilidad para que los interesados puedan comprender dichos textos sin tener que contar con unos conocimientos específicos en la materia.

A pesar de que todavía queda mucho por mejorar en la materia, como indican los propios legisladores, este Reglamento ha supuesto un gran cambio para el ámbito de la protección de datos en la UE.

En todo caso, todas y cada una de las disposiciones que contiene el RGPD son directamente aplicables en los Estados miembros de la UE sin necesidad de trasposición, al contrario de lo que ocurría con la anterior Directiva, que necesitaba de un complemento normativo de los Estados para su efectiva implementación, a lo cual se denomina jurídicamente "transposición" al Derecho interno o nacional.

De lo anterior podemos comprobar que frente a la ya derogada directiva que lo que intentaba era una mera armonización, en la actualidad se ha optado por una unificación normativa a través del **RGPD,** el cual está llamado a sustituir a las legislaciones nacionales salvo en aspectos determinados los cuales prevé explícitamente el Reglamento, indicando que sus normas pueden ser especificadas o restringidas por los Estados miembros, como podemos comprobar en su ***art. 8*** *sobre la edad aplicable al consentimiento de los menores.*

Finalmente, tras la unificación a través de un Derecho uniforme, como regla general no resultará necesario en las situaciones intracomunitarias determinar la legislación de qué concreto Estado miembro es aplicable como ocurría con la directiva y como ocurre en el caso Weltimmo, respecto a las materias objeto del **RGPD**.

b) Comité Europeo de Protección de Datos (CEPD)

Se trata de un organismo independiente, que se encargara de garantizar el cumplimiento del **RGPD** en los Estado Miembros, así como de promover la cooperación entre las autoridades de protección de datos de la **UE**.

El **CEPD** este compuesto por distintos representantes de las autoridades nacionales de cada Estado miembro y del Supervisor Europeo Protección de Datos.

Desde dicho organismo pueden adoptar **directrices generales** para clarificar los términos de la legislación europea de protección de datos, proporcionando a todas las partes interesadas una interpretación coherente de sus derechos y obligaciones.

Además, se encuentran habilitados por el propio **RGPD** para tomar **resoluciones vinculantes** con respecto a las autoridades nacionales de supervisión para garantizar una aplicación coherente de la normativa.

3.2.2. Normativa en España

a) Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Tras años de elaboración la **LOPDGDD** entro en vigor en España el 7 de diciembre de 2018, ha sido creada a efectos de adaptar la legislación española al Reglamento General de Protección de Datos de la Unión Europea.
El principal objeto, a parte de lo indicado en el párrafo anterior es cumplir con *el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el* ***artículo 18.4 de la Constitución***, así como garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el **artículo 18.4 de la Constitución**.
Es preciso señalar también el ámbito de aplicación de la presente Ley:
En primer lugar, se aplica para todos los datos personales registrados en un soporte físico que permita su tratamiento.
Asimismo, se aplicará a todos los tratamientos de datos que se realicen dentro del territorio español, también será aplicable cuando el responsable de los datos se encuentre fuera de la UE y trate datos ubicados en territorio español, como excepción si estos se utilizan solamente con fines de tránsito.

Por otra parte, al igual que se ha indicado en el punto anterior, en lo que respecta al órgano público de control de cumplimiento de dicha normativa con carácter general en España, éste no ha cambiado a pesar de que la normativa aplicable sí que haya sido actualizada sigue siendo como anteriormente la Agencia Española de Protección de Datos (AEPD).
También se considera necesario en este punto hacer referencia a los ámbitos más comunes de actuación de dicho organismo independiente:

- Internet y Redes Sociales.
- Reclamaciones de telecomunicaciones.
- Publicidad no deseada.
- Educación y menores.
- Videovigilancia.
- Proyectos Europeos.

A modo de cierre no puede finalizar este punto sin indicar que la AEPD puede actuar tanto de oficio como a instancia de parte (por denuncia de los afectados).[5]

3.3. JURISPRUDENCIA

En este punto nos vamos a centrar en analizar la jurisprudencia más relevante que tenga especial conexión con el caso *"Weltimmo"*. Dado que nos encontramos ante una resolución sobre un tema bastante controvertido, en este caso solamente hemos de hacer referencia a una ST que tenga especial relación;

3.3.1. Sentencia del TJUE 13-5-14, asunto C-131/12, Google Spain, S.L., Google Inc. vs Agencia Española de Protección de Datos (AEPD) - *Caso Google Spain y Google contra AEPD y Costeja* -.[6]

El Tribunal de Justicia de la Unión Europea (TJUE), dictamino a petición de la Audiencia Nacional, por primera vez en este conocido caso el "derecho al olvido" en internet.
La presente Sentencia se posiciona como un hito en lo que respecta a la defensa de la privacidad de los ciudadanos, esto es así, dado que a través de esta resolución se abren las

[5] < https://www.aepd.es/es>

[6] **ÁLVAREZ CARO, MARIA (2015):** *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital.* ISBN:978-84-290-1836-3

puertas para que todos los ciudadanos puedan reclamar tanto a Google como a otros buscadores la eliminación de los enlaces donde aparece su información personal.

A través de esta Sentencia se resuelve la demanda interpuesta por Mario Costeja, el cual había sufrido un embargo por parte de la Seguridad Social, que ya había sido resuelto y liquidado por su parte, aun así, esta noticia seguía apareciendo en el buscador de Google, exactamente en una noticia de La Vanguardia, de tal manera que se le estaba causando al demandante un grave perjuicio para su reputación.

A lo anterior el TJUE indico lo siguiente:

"Si a raíz de la solicitud de la persona afectada se comprueba que la inclusión de esos enlaces en la lista es incompatible actualmente con la directiva (de protección de datos personales), la información y los enlaces que figuran en la lista deben eliminarse".

Concluyendo en su Sentencia:

Que si «el gestor de un motor de búsqueda en internet es responsable del tratamiento que aplique a los datos de carácter personal que aparecen en las páginas web publicadas por terceros" este deberá de respetar la **Directiva 95/46** en materia de protección de datos.

Por lo tanto, de lo indicado por el TJUE se concluye que los interesados podrán solicitar el ejercicio de su *derecho al olvido*[7] directamente motor de búsqueda como responsable del tratamiento, ósea, en este caso a *Google Spain*, en vez de al tercero que ha publicado en su página (La Vanguardia). En el caso de que el interesado no vea su derecho atendido, este podrá instar tanto a los Tribunales como a la AEPD para que realicen las actuaciones oportunas a fin de conseguir el ejercicio de del derecho al olvido de un ciudadano.

Finalmente, el fallo del TJUE indica, que, a pesar de fijar doctrina para casos del estilo, todos han de ser examinados minuciosamente para poder aplicar el mismo criterio que se ha seguido en el caso *Google Spain*. Mientras que el abogado general del TJUE, dio la razón a Google, concluyendo que "los servicios de motor de búsqueda en Internet no son responsables de los datos personales incluidos en las páginas web que tratan".

Pero ¿Cuál es la relación del caso Google Spain con el Caso Weltimmo?

El TJUE en el caso Weltimmo utiliza como base el caso *Google Spain*, dado que en este ya se había analizado en las cuestiones prejudiciales lo relativo a la interpretación del art. 4.1.a) de la Directiva, de tal manera que se establecen tanto el concepto de "establecimiento" en

[7] **Derecho al olvido según la AEPD:** "el **derecho** que tiene un ciudadano 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." < https://www.aepd.es/es>

relación con la **Directiva 95/46**, así como la determinación de si el tratamiento de datos se produce "en el marco de las actividades de dicho establecimiento".
En pocas palabras, en ambas Sentencias se trata tanto el ámbito de aplicación tanto material como territorial de la **Directiva 95/46**.

4. FUNDAMENTOS DE DERECHO

Antes de centrarnos en los fundamentos en sí haremos una breve referencia a los distintos puntos o elementos de conexión que se han de tener en cuenta en el ámbito del derecho internacional privado:
Dichos vínculos de conexión son las circunstancias que se tienen en cuenta para determinar si la ley aplicable será la de un país o la de otro, por ejemplo:

- ✓ Nacionalidad de una persona (lex patriae)
- ✓ Domicilio o residencia habitual (lex domicilii)
- ✓ La sede en el caso de una persona jurídica (lex rei sitae)

4.1. ¿Qué vínculos territoriales considera relevantes el tribunal y con que alcance?

a) El lugar del establecimiento del gestor de los datos

Una de las partes en la que más énfasis muestra el TJUE es en la determinación del ***"establecimiento"*** del responsable del tratamiento (en este caso Weltimmo), esto se estima necesario debido a lo que indica el *artículo 4.1.a) de la Directiva 95/46*:

"Derecho nacional aplicable

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios

Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable".

Como podemos comprobar con su lectura, se desprende la necesidad de esclarecer que se considera establecimiento, para lo cual tanto el TJUE como el Abogado General en sus conclusiones (25 junio de 2015), dejan establecido el criterio de que si atendemos al considerando 19 de la Directiva 95/46 hemos de enfocar el criterio de establecimiento desde un ***punto de vista flexible del concepto***, de tal manera que el establecimiento de un responsable del tratamiento no va a ser solamente donde tenga su domicilio social, sino que también se puede extender tal y como indica la Sentencia a cualquier actividad real y efectiva, por mínima que sea, ejercida mediante una instalación estable.

Consecuentemente, por todo lo expuesto el TJUE considera relevante el vínculo territorial del lugar del establecimiento del gestor de los datos. Esto es así, dado que si una entidad cuenta con un establecimiento en un Estado Miembro y tal y como se indica en **el art.4.1.a) de la Directiva 95/46** ha de cumplir con la normativa en materia de protección de datos de dicho Estado. No todo queda aquí, también nos indica el TJUE que una entidad ***podrá ser sancionada por la autoridad de control competente***, en lo que respecta al tratamiento de datos que se realiza en el establecimiento del estado y por incumplimiento de su normativa nacional.

b) El lugar de gestión o de transmisión de los datos

EL TJUE como ya declaro en su *Sentencia Google Spain* (131/12, EU:C:2014:317, apartado 52), que de los dispuesto en el **art. 4.1.a) de la Directiva** no se desprende la exigencia de que el tratamiento sea efectuado por el propio establecimiento en cuestión, si no que puede realizarse en el marco de actividades de éste.
Es de suma importancia añadir que en el litigio principal del caso Weltimmo nos encontramos con que **el tratamiento de datos de carácter personal se realiza a través de páginas de internet,** es decir con la publicación de los datos de los interesados en dichas plataformas. Entonces en este punto es interesante hacerse la siguiente pregunta:

¿Se considera lo descrito un tratamiento de datos de carácter personal propiamente dicho?

Para dar respuesta a esta pregunta, hemos de dirigirnos al ap.37 de la Sentencia Weltimmo:

"A este respecto, es preciso recordar que, en lo que atañe concretamente a Internet, el Tribunal de Justicia ya ha tenido ocasión de declarar que la conducta que consiste en hacer referencia, en una página de Internet, a datos personales debe considerarse un «tratamiento» en el sentido del artículo 2, letra b), de la Directiva 95/46 (sentencias Lindqvist, C-101/01, EU:C:2003:596, apartado 25, y Google Spain y Google, C-131/12, EU:C:2014:317, apartado 26)."

El considerarlo como un tratamiento de datos de carácter personal, ayuda al TJUE para considerar el tratamiento como efectuado dentro del marco de las actividades del establecimiento que se ha determinado en base al **art. 4.1.a) de la Directiva** y así poder dilucidar la aplicación al litigio principal del Derecho Húngaro, ya que el tratamiento de datos se considera realizado en el establecimiento de dicho país.

De lo anterior se concluye que el TJUE considera relevante el presente vinculo para poder determinar el derecho nacional aplicable al caso.

c) El lugar de localización del servidor

Respecto de este elemento, fue considerado determinantes y ha sido apuntado por el Grupo del artículo 29 en relación con los motores de búsqueda, pudiendo resultar de utilidad para la determinación de si las actividades se sitúan en el contexto del establecimiento: el hecho de que el establecimiento sea responsable de las relaciones con los usuarios; que participe en la venta de publicidad orientada a los habitantes de este Estado o que responda ante las autoridades competentes de un Estado miembro respecto a los datos de los usuarios.

Por lo tanto, si el servidor se encuentra en un Estado puede ayudar para probar que la actividad efectiva y real de la entidad se realiza en dicho estado y por lo tanto su establecimiento se encuentra allí.

De tal manera, que esta premisa también se considera importante a efectos de determinar la ley aplicable en el caso.

d) El lugar de situación de los inmuebles de las transacciones

Por lo que respecta al lugar de situación de los inmuebles, en el presente caso, se encuentran en Hungría.
El TJUE indica textualmente:

"por un lado, que la actividad del responsable de dicho tratamiento, en cuyo marco éste tiene lugar, consiste en la gestión de sitios de Internet de anuncios de inmuebles situados en el territorio de dicho Estado miembro y redactados en la lengua de ese Estado y que, en consecuencia, se dirige principalmente, incluso íntegramente, a dicho Estado miembro y, por otro lado, que ese responsable dispone de un representante en el referido Estado miembro que se encarga de cobrar los créditos resultantes de dicha actividad y de representarlo en los procedimientos administrativo y judicial relativos al tratamiento de los datos en cuestión".

De lo anterior se puede interpretar que para el TJUE al igual que el resto de las premisas incluidas en el párrafo anterior, el hecho de que los inmuebles que son objeto de las transacciones son una parte necesaria para determinar donde se realiza la actividad principal del responsable del tratamiento y así poder determinar la ley aplicable a esa actividad.
Como conclusión, en el caso Weltimmo, al determinarse que la actividad principal se realiza en Hungría y además el establecimiento se encuentra allí, el derecho aplicable al caso será el nacional de Hungría.

e) El lugar de residencia de los propietarios de los bienes

En este caso, el **TJUE** considera la *lex domicilii* de los propietarios de los bienes como uno de los puntos a tener en cuenta para determinar la ley aplicable al caso, de tal manera que estos son los que inician las actuaciones ante la autoridad húngara.

Esto es así, de tal manera que toda la actuación se inició debido a que la mayoría de los propietarios de los bienes que se anunciaban en el sitio web de Weltimmo cuentan con la residencia húngara, por lo que estos acudieron a la autoridad de control húngara para realizar dicha reclamación al respecto.

4.2. ¿Qué relevancia tendría el criterio de la nacionalidad en el caso a la luz de la decisión del TJUE?

Respecto de la conexión personal entendida como nacionalidad (*lex patriae*) y como el **TJUE** indica en su Sentencia, se puede ver que se considera irrelevante como factor a valorar la nacionalidad de las personas afectadas en el caso, lo cual podemos comprobar con frases de su Sentencia:

"En cambio, es irrelevante el tema de la nacionalidad de las personas afectadas por dicho tratamiento de datos".

Como conclusión, se desprende de párrafos como este, que para el **TJUE** la nacionalidad o de los propietarios de los bienes no es objeto de controversia, dado que no es determinante para poder valorar el derecho aplicable al caso. Como nos indica el propio tribunal, este aspecto junto con otros como el lugar desde donde se hayan cargado los datos, no tienen, a este respecto, una incidencia directa y determinante en la fijación del derecho aplicable. En efecto, dichos elementos no figuran en la Directiva en tanto que criterios pertinentes que permitieran apartarse del criterio establecido por el *artículo 4, apartado 1, letra a).*

4.3. ¿Hasta dónde alcanza el límite de la competencia de autoridad en el caso? ¿Le parece razonable?

En relación con la competencia de la autoridad en el presente caso, el **TJUE** nos hace las siguientes indicaciones:
Hemos de partir del análisis del *artículo 28.6 de la Directiva 95/46* **:**
"6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro."

Es decir, en principio hemos de partir de la teoría de que toda autoridad de control es competente para ejercer sus potestades dentro del territorio nacional del que forme parte.

Además, en el caso de que sea otro derecho el que se aplique al caso, dicha autoridad de control podrá tener competencias en el caso si ésta es instada por parte de la autoridad del Estado Miembro del que es aplicable el derecho nacional, *pero nunca tendrá la potestad sancionadora, como veremos más adelante.*

Para poner lo dispuesto de manifiesto el caso que nos atañe, aunque el derecho aplicable al caso fuese el derecho de Eslovaquia, la autoridad de control húngara podría ejercer sus potestades si fuese instada a actuar por parte de la autoridad de Eslovaquia.

El **TJUE** para dilucidar este asunto, ha seguido las directrices recomendadas por el Abogado General del caso en su informe de conclusiones (25 de junio de 2015), en el cual indica que la utilización como regla general del criterio en el que exista correlación entre ley aplicable y autoridad nacional de control competente. Por lo cual, la capacidad de actuación de la autoridad nacional de control será limitada en el caso de que el derecho que se aplique sea el de otro país distinto al suyo.

En resumen, la autoridad de control en el caso de que el derecho aplicable sea el de otro país distinto al que pertenece, podrá instar labores de investigación, pero nunca podrá sancionar, lo que deberá hacer es informar a la autoridad de control competente (del país de donde sea aplicable el derecho nacional) para que esta pueda interponer las sanciones oportunas.

Finalmente, bajo mi punto de vista, tanto la explicación que realiza el **TJUE** como el **Abogado General** del caso al respecto de los límites de la autoridad me parecen totalmente fundamentados. Por lo tanto, estoy de acuerdo con lo indicado, esto es así porque no me parecería coherente que una autoridad de control, la cual presta sus funciones dentro de un territorio nacional pueda sancionar en base al derecho nacional de otro Estado. Dicha autoridad no tiene por qué conocer el derecho de otro Estado miembro y además en el caso de que lo conozca al no manejarlo continuamente probablemente sea más complicado el sancionar en base a ese derecho. De tal manera que si cada autoridad de control sanciona en base al derecho nacional de su Estado seguramente tengamos más seguridad jurídica. Además, como ya se ha indicado en puntos anteriores si esto se llevase a cabo no se estaría cumpliendo con el principio de soberanía territorial ni con el principio de

legalidad.

Para concluir, lo que sí que me parece interesante es que la autoridad competente del estado donde sucedan los hechos pueda realizar labores de investigación para posteriormente poder facilitárselas a la autoridad que sancionara finalmente el caso.

Por todo lo anterior, mi opinión es totalmente favorable para lo indicado en este apartado por parte del Tribunal.

5. CONCLUSIONES

PRIMERA. – Tras realizar un análisis profundo de la **ST Weltimmo** y de sus antecedentes, se puede observar la complejidad con la que cuenta la materia de protección de datos y en especial cuando nos encontramos ante la determinación de la ley aplicable y la autoridad competente al caso. Para ayudar a resolver la complejidad hemos de interpretar tanto la **Directiva 95/46** como los dictámenes al respecto emitidos por el **GT29**.

El litigio principal se refiere a una controversia entre la autoridad de control húngara en materia de protección de datos y la empresa *Weltimmo*, la cual tiene domicilio social en Eslovaquia y gestiona una página web que se dedica a temas inmobiliarios. Los inmuebles anunciados en dicha web se encuentran en Hungría, de tal manera que algunos de los dueños de estos son residentes en dicho país. Por lo que deciden presentar una reclamación ante dicha autoridad húngara, la cual sanciono a *Weltimmo*.

En Sentencia del **TJUE** se intenta determinar cuál es la ley aplicable al caso y qué autoridad de control es la competente.

SEGUNDA. – Para determinar la ley aplicable al caso primero parte el **TJUE** de examinar si existe un "establecimiento", además de un ejercicio efectivo y real por parte de Weltimmo en Hungría. De acuerdo con la Jurisprudencia previa al caso *Weltimmo* (como es la Sentencia *Google Spain*) se confirma por parte del **TJUE** que hacer referencia a datos de carácter personal en una página web se considera como un tratamiento de estos, además se engloba este tratamiento dentro de la actividad de la entidad.

TERCERA. - Como factores determinantes para apreciar si en un caso como *Weltimmo* se puede considerar la existencia de un "establecimiento" a efectos del **artículo 4.1.a) de la Directiva 95/46** entiende relevantes tanto el hecho de que Weltimmo cuente con un representante en Hungría, así como que la sociedad abrió una cuenta bancaria en la ciudad, junto con que utiliza el apartado de correos húngaro para la gestión de sus asuntos bancarios.

De lo indicado se desprende que una sociedad como *Weltimmo* pueda considerarse establecida en un Estado distinto a aquel en el que tiene su domicilio social. De todo lo indicado se desprende que Weltimmo tiene su domicilio social en Eslovaquia, pero es considerado por el **TJUE** que existe un "establecimiento" de dicha sociedad en Hungría.

CUARTA. – En virtud del **artículo 4.1.a) de la Directiva 95/46 y en lo que respecta a la determinación de la ley aplicable,** cuando se determina que una sociedad cuenta con un establecimiento en un Estado Miembro distinto al que tiene su domicilio social debe de cumplir con la legislación en materia de protección de datos del Estado en el que tenga su establecimiento. Por lo cual, se determina que la ley aplicable al caso *Weltimmo* sería la ley nacional húngara, dado que su establecimiento se encuentra en dicha ciudad.

Por lo expuesto, podemos comprobar el elevado nivel de protección con el que contaba la Directiva, la cual ya no se encuentra en vigor y se ha visto derogada por el nuevo Reglamento Europeo en materia de protección de datos (**RGPD**).

QUINTA. – Una vez determinada la ley aplicable al caso *Weltimmo*, otra de las cuestiones prejudiciales planteadas al TJUE es la autoridad competente, para lo cual el Tribunal realiza la interpretación del **artículo 28.6 de la Directiva 95/46,** atendiendo a esta premisa se determina que toda autoridad de control será competente independientemente del derecho aplicable, para actuar en el territorio de su propio Estado. Si bien es cierto, se hace referencia a los poderes que tendrá dicha autoridad de control (**art. 28.3 Directiva 95/46**), que son entre otros el de investigación e intervención y es aquí donde encontramos la *especificidad del caso.*

Finalmente, el TJUE determina al igual que lo hace el abogado general en su informe que la capacidad de actuación de la autoridad de control de un Estado miembro cuando resulte aplicable la ley nacional de otro Estado miembro es

limitada, dichas limitaciones las encontramos en lo relativo a las sanciones, dado que una autoridad de control no podrá interponer sanciones fuera del territorio de su propio Estado, de tal manera que si esto sucede deberá de instar a la autoridad de control **de el Estado Miembro del que sea de aplicación el Derecho nacional.**

SEXTA. – Atendiendo tanto a la normativa y a la jurisprudencia al respecto podemos comprobar que a partir del caso *Weltimmo* queda determinado que, si una entidad se considera establecida en Estados miembros distintos de aquel en el que tenga su domicilio social, ésta ha de cumplir también con la legislación nacional sobre protección de datos del Estado miembro en el que quede demostrado que tiene establecimiento.
Asimismo, respecto de la capacidad de la autoridad de control que reciba una denuncia, en el caso de que se de lo indicado en el párrafo anterior queda limitada, de tal manera que no podrá sancionar si el Derecho aplicable al caso es el de otro Estado miembro que difiere del suyo.

SEPTIMA. – En la actualidad, con la plena aplicación del **RGPD** y la derogación de la **Directiva 95/46** el problema de la determinación de la ley aplicable al caso no tendría lugar, puesto que contamos con una norma jurídica de derecho comunitario con alcance general y eficacia directa como es el Reglamento. Por lo cual, como podemos comprobar cada vez se va actualizando a los nuevos tiempos y a las nuevas controversias la normativa en materia de protección de datos.

6. BIBLIOGRAFIA

➢ Libros y Revistas Jurídicas:

- **PALOMAR OLMEDA, Alberto (2018):** *Prácticum. Ejercicio de la Abogacía 2019*. Thomson Reuters.
- **DE MIGUEL ASENSIO, Pedro Alberto (2014):** *El tratamiento de datos personales por buscadores de Internet tras la sentencia Google Spain del Tribunal de Justicia.* Dialnet. ISSN-e 2255-551X
- **APARICIO SALOM, Javier (2019)**: *Estudio sobre la protección de Datos 2019. Aranzadi.*
- **DE MIGUEL ASENSIO, Pedro Alberto (2015):** *Aspectos internacionales de la protección de datos: Las Sentencias Schrems y Weltimmo del TJUE*. Dialnet. ISSN-e 2255-551X
- **MEMENTO PRÁCTICO SOBRE PROTECCIÓN DE DATOS (2019-2020).** Lefebvre.
- **ÁLVAREZ CARO, MARIA (2015):** *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital.* ISBN:978-84-290-1836-3

➢ Consultas Web:

- **CANDELA PÉREZ, Ana (27.10.2015):** *Comentario al asunto C-230/14, "Weltimmo".* Lvcentinvs. <http://www.lvcentinvs.es/2015/10/27/post-invitado-comentario-al-asunto-c%E2%80%9123014-weltimmo/>.

- **DE MIGUEL ASENSIO, Pedro Alberto (enero-junio 2017):** *Competencia y Derecho aplicable en el RGPD sobre protección de datos en la UE.* Biblioteca de Cultura Jurídica. <http://bibliotecaculturajuridica.com/EDIT/1665/competencia-y-derecho-aplicable-en-el-reglamento-general-sobre-proteccion-de-datos-de-la-union-europea.html/>.

- **ÚRBAN, Daniel (08.10.2015):** *Nueva Sentencia del TJUE sobre el tratamiento intracomunitario de datos personales.* Blog Cuatrecasas. <https://blog.cuatrecasas.com/propiedad-intelectual/tratamientos-intracomunitarios-de-datos-personales-nueva-sentencia-del-tjue/>.

➢ Jurisprudencia:

- STJUE de 1 de octubre (*C-230/14*; Weltimmo s.r.o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság) *"Caso Weltimmo".*

- STJUE de 25 de julio (*C-362/14;* Maximillian Schrems y Data Protection Commissioner, con intervención de: Digital Rights Ireland Ltd) *"Caso Schrems".*

- STJUE de 13 de mayo (*C 131/12: Google Spain y AEPD, Mario Costeja***)** *"Caso Google Spain".*

- SJUE de 6 de noviembre (C-101/01: Agencia Sueca **"Datainspektion**" contra Bodi Lindqvist) *"Caso Lindqvist".*

- Dictamen 8/2010 sobre ley aplicable, emitido por el GT29 Dictamen 8/2010 del 16 de diciembre de 2010, sobre el Derecho aplicable, emitido por el Grupo de

Protección de Datos del Artículo 29.

- Informe de Conclusiones del Abogado General Pedro Cruz Villalón presentadas el 25 de junio de 2015 (Asunto C-230/14) *"Caso Weltimmo"*.

➢ Legislación:

- Constitución Española de 1978.
- 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.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales.

- Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH).