ASPECTOS INTERNACIONALES DE LA PROTECCIÓN DE DATOS: LAS SENTENCIAS SCHREMS Y WELTIMMO DEL TRIBUNAL DE JUSTICIA

Pedro Alberto DE MIGUEL ASENSIO *

Publicado en:

La Ley Unión Europea

Número 31 – Noviembre de 2015,
pp. 1-10

ISSNe: 2255-551-X

(*Diario La Ley*, ISSN 1989-6913, Nº 8656, 2015)

* Catedrático de Derecho internacional privado
Facultad de Derecho
Universidad Complutense de Madrid
E- 28040 MADRID
pdmigue@der.ucm.es

Resumen: Análisis de dos recientes sentencias del Tribunal de Justicia de gran importancia en relación con los aspectos internacionales de la protección de datos personales. La sentenicia Schrems declara la invalidez de los principios de puerto seguro, un mecanismo fundamental del entramado que facilitaba las transferencias internacionales de datos desde la UE a EEUU, al que han venido estando adheridas los principales prestadores de servicios de Internet, como redes sociales, correo electrónico o motores de búsqueda. Por su parte, en la sentencia Weltimmo el Tribunal de Justicia realiza importantes precisiones en materia de determinación de la ley aplicable al tratamiento de datos personales en páginas de Internet, así como con respecto a la concreción de la autoridad competente para investigar y sancionar esas conductas.

Palabras clave: protección de datos, transferencias internacionales, ley aplicable, autoridad competente

Abstract: This article focuses on two recent judgments by the Court of Justice of the EU of great significance regarding certain international aspects of data protection law. The Schrems judgment declares invalid the Safe Harbour Principles, a key instrument to facilitate the transfer of data from the EU to the US. The main providers of Internet services, such as social networks, e-mail and search engines had adhered to this mechanism. The Weltimmo judgment includes relevant approaches regarding the determination of the applicable law to the processing of data in Internet web sites and with respect to the powers of national authorities in cross-border situations within the EU.

Keywords: data protection, international transfers, applicable law, competence

Pedro A. De Miguel Asensio
"Aspectos internacionales de la protección de datos:
las sentencias Schrems y Weltimmo del Tribunal de Justicia",
La Ley Unión Europea, Número 31, 2015, pp. 1-10.

Aspectos internacionales de la protección de datos: las sentencias *Schrems* y *Weltimmo* del Tribunal de Justicia

Pedro Alberto De Miguel Asensio
Catedrático de Derecho internacional privado
Universidad Complutense de Madrid

I. Introducción

Dos sentencias pronunciadas por el Tribunal de Justicia en este mes de octubre presentan particular interés desde la perspectiva internacional de la protección de datos personales. Singular repercusión, por su gran trascendencia ha alcanzado la STJ de 6 de octubre de 2015, C-362/14, *Schrems*, que concluye con la declaración de invalidez de la Decisión 2000/520/CE de la Comisión relativa a los principios de puerto seguro, hasta ahora pieza fundamental del entramado que facilitaba las transferencias internacionales de datos desde la UE a EEUU, resultando bien conocido el extraordinario crecimiento de las transferencias transatlánticas de datos personales en el contexto de Internet. Entre las empresas adheridas al sistema de los principios de puerto seguro se incluyen los principales prestadores de servicios de redes sociales, motores de búsqueda y correo electrónico, respecto de los que resulta especialmente preocupante las revelaciones acerca de su eventual conexión con los programas de supervisión del Gobierno de EEUU. En el complejo y lento proceso de revisión de la legislación europea de protección de datos, la sentencia presenta un gran interés, al tiempo que contribuye una vez más a poner de relieve cómo esos prestadores de servicios han venido tradicionalmente operando en la UE sin que el restrictivo marco formalmente instaurado en la UE les haya sido aplicado. Ciertamente, la declaración de invalidez resulta de singular trascendencia en un contexto en el que las tradicionales carencias en la aplicación efectiva por las autoridades europeas (básicamente, nacionales) a ciertos prestadores de servicios procedentes terceros Estados de la rigurosa legislación europea sobre protección de datos, unidas a ciertas prácticas de autoridades y empresas de EEUU, han generado no sólo importantes riesgos (vulneraciones) del derecho fundamental a la protección de datos de los afectados sino que han constituido también

un factor muy acusado de desventaja competitiva para las empresas europeas en el ámbito de la sociedad de la información.

Desde la perspectiva de la deficiente aplicación de la normativa europea sobre protección de datos personales -como reflejan también las circunstancias del litigio principal en el asunto *Schrems*-, el reforzamiento de la posición de las autoridades de control reviste gran importancia. Aunque se trata de una cuestión llamada a evolucionar en el proyectado reglamento general sobre protección de datos de la UE, la sentencia de 1 de octubre de 2015, C-230/14, *Weltimmo* reviste gran interés. El Tribunal de Justicia realiza importantes precisiones en materia de determinación de la ley aplicable al tratamiento de datos personales en páginas de Internet, así como con respecto a la concreción de la autoridad competente para investigar y sancionar esas conductas. La sentencia *Weltimmo* refuerza la posibilidad de actuación por parte de las diversas autoridades nacionales de control (así como facilita el acceso por los afectados a la de su propio Estado) en situaciones en las que prestadores de servicios en principio establecidos en un único Estado miembro (o en un tercer Estado, como EEUU) tienen un gran número de usuarios en diversos Estados miembros en los que además cuentan con algún tipo de presencia, como una mera oficina de representación, de modo que a efectos de la aplicación de la legislación de protección de datos (y de la determinación de la autoridad de control) se les puede considerar establecidos en más de un Estado miembro.

II. La sentencia *Schrems* y la declaración de invalidez de los principios de puerto seguro

1. Los principios de puerto seguro: fundamento y cuestionamiento

Con respecto a los principios de puerto seguro, cabe reseñar que constituyen un peculiar mecanismo, fruto de una prolongada negociación entre la Comisión y el Gobierno de EEUU, recogido en la Decisión de la Comisión 2000/520/CE de 26 de julio de 2000. Se trata de un instrumento singular que, tomando en consideración el contraste entre la autorregulación estadounidense y los estrictos criterios legales en materia de protección de datos de la UE, permite a las entidades de EEUU que lo deseen

comprometerse a su cumplimiento, lo que tiene como consecuencia fundamental que respecto de las transferencias de datos personales dirigidas a esos concretos destinatarios se considera que EEUU es un país que proporciona protección adecuada por lo que, desde la perspectiva española, aunque no concurran las excepciones del artículo 34 LOPD, deja de ser necesaria para esas transferencias internacionales de datos la previa autorización de la Agencia Española de Protección de Datos, si bien será preciso acreditar ante la AEPD que el destinatario se encuentra entre las entidades que se han adherido a los Principios así como que se encuentra sometido a la jurisdicción de uno de los organismos públicos de EEUU que figuran en la mencionada Decisión 2000/520/CE. Además, la AEPD tiene la facultad de suspender las transferencias a empresas adheridas a los Principios en supuestos específicos, si bien la Comisión manifiesta que hasta la fecha no le consta que ninguna autoridad de un Estado miembro haya adoptado esa medida desde el inicio de la aplicación de los Principios. En todo caso, resulta claro que es un mecanismo que facilita las transferencias de datos a EEUU, en comparación con el resto de países del mundo que no proporcionan un nivel adecuado de protección de datos personales para la UE.

Ilustrativo de la ineficacia de la política de la UE en materia de protección de datos –tanto desde la perspectiva de la tutela de este derecho fundamental como de la protección de los intereses de las empresas y consumidores europeos en el ámbito de la sociedad de la información- es que la sentencia *Schrems* funda en buena medida la declaración de invalidez de la Decisión 2000/520/CE de la Comisión relativa a los principios de puerto seguro, en las conclusiones alcanzadas por la propia Comisión hace ya un par de años, en su Comunicación sobre el funcionamiento de los principios de puerto seguro desde la perspectiva de los ciudadanos y empresas de la UE [COM(2013) 846 final], en el sentido de que ese mecanismo facilitaba la vulneración sistemática de los estándares de protección de la legislación europea con respecto a datos personales transferidos desde la UE a EEUU por empresas adheridas al sistema de los principios de puerto seguro. Ciertamente, en ese documento la Comisión destacaba la negativa repercusión de la situación existente sobre la competitividad de las empresas europeas, constataba un significativo nivel de incumplimiento de los principios de puerto seguro,

al tiempo que ponía de relieve su voluntad de revisarlo para dotarlo de una mayor eficacia, como opción preferible frente a la suspensión o revocación de este sistema, habida cuenta de los perjuicios que de tal opción derivarían para los intereses en EEUU y la UE de las empresas participantes en el mismo.

También había puesto entonces de relieve la Comisión cómo la conexión con los programas de supervisión del Gobierno de EEUU de los principales prestadores de servicios de Internet era elemento que menoscababa la confianza en esos servicios de los ciudadanos europeos (cuyas comunicaciones y datos no gozan en el ordenamiento de EEUU de una protección frente a esas actividades de supervisión por las autoridades de EEUU similar a la de los residentes en EEUU). En este sentido, la Comisión había destacado que en la medida en que los programas de supervisión estadounidenses afecten a datos almacenados en la nube a los que resulte de aplicación la legislación europea sobre protección de datos personales, la facilitación a las autoridades de EEUU -sin cumplir los requisitos previstos en la legislación europea y nacional aplicable- del acceso a los datos ahí alojados, incluso por quienes revistan la condición de meros encargados del tratamiento, supondrá típicamente la infracción de la legislación europea de protección de datos –COM(2013) 846 final, p. 6-, sin que las excepciones previstas en el marco de los principios de puerto seguro permitan alcanzar normalmente una conclusión diferente –COM(2013) 847 final, pp. 16-17-.

Aunque el detonante en este caso que lleva a liquidar el sistema de los Principios de puerto seguro tal como fue instaurado por la Decisión 2000/520/CE es el que ésta ha permitido en la práctica una vía de acceso a las autoridades de inteligencia de EEUU para recopilar masivamente datos personales transferidos a EEUU desde la UE en virtud de tales Principios, lo cierto es que las constataciones de la propia Comisión pusieron de relieve que el sistema ha hecho posible el tratamiento en EEUU por esas mismas empresas de datos de sus usuarios en la UE sin controles efectivos de respeto a los estándares europeos de protección de datos, habiéndose comprobado que un número elevado de empresas participantes no respetaban en la práctica los principios de puerto

seguro, lo que no impidió que el sistema siguiera funcionando (ap. 21 de la sentencia *Schrems*).

2. Régimen de las transferencias internacionales de datos

En el marco de la Directiva 95/46 sobre protección de datos personales, el criterio de base es que las transferencias internacionales de datos personales desde la UE a terceros Estados que no garanticen un nivel de protección adecuado (art. 25) requieren autorización previa, salvo que concurra alguna de las excepciones previstas en el artículo 26.1 de la Directiva (consentimiento inequívoco del afectado a la transferencia; que la transferencia sea necesaria para la ejecución de un contrato entre interesado y responsable; que sea necesaria para la salvaguardia de un interés público importante o el ejercicio de un derecho en un proceso; que sea necesaria para la salvaguardia de un interés vital del interesado; o que la transferencia tenga lugar desde un registro público cuando concurran determinadas circunstancias). Habida cuenta de que la obtención de autorización o del consentimiento inequívoco del afectado a la transferencia constituye un obstáculo práctico relevante, que se subordina además a la prestación de garantías suficientes por parte del responsable –típicamente, mediante la inserción de ciertas cláusulas contractuales en sus relaciones con el destinatario de los datos-, el mecanismo de los principios de puerto seguro ha resultado fundamental para facilitar la transferencia de datos personales de la UE a EEUU.

Con respecto al funcionamiento de los artículos 25, 26 y concordantes de la Directiva, la principal aportación de la sentencia *Schrems* es que si bien cuando la Comisión ha adoptado una decisión que constata que un tercer país garantiza un nivel de protección adecuado –como sucede con la relativa al puerto seguro con respecto a EEUU- los Estados miembros y las autoridades nacionales de control no pueden adoptar medidas contrarias a la decisión, como establecer que el país en cuestión no garantiza un nivel de protección adecuado, sí cabe que la autoridad nacional de control conozca de reclamaciones relativas al tratamiento de datos transferidos con base en la decisión de la Comisión y que la validez de ésta sea revisada por el Tribunal de Justicia en el

marco de una cuestión prejudicial planteada por un tribunal nacional derivada de una de esas reclamaciones, como sucede con los tribunales irlandeses en el asunto *Schrems*.

3. Invalidez de los principios de puerto seguro

Elementos determinantes para la declaración de invalidez de la Decisión 2000/520/CE por el Tribunal de Justicia, en gran medida en línea con la propuesta del Abogado General son los siguientes. El sistema de autocertificación instaurado carece de la necesaria fiabilidad, en la medida en que los principios de puerto seguro son aplicables únicamente a las entidades estadounidenses autocertificadas pero las autoridades de EEUU no quedan sometidas a esos principios, sin que la Decisión establezca cómo los EEUU a la luz de su legislación interna o sus compromisos internacionales garantizan esos principios (aps. 82-83 de la sentencia). La Decisión 2000/520/CE reconoce la primacía de las "exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]" sobre los principios de puerto seguro (ap. 84) en términos que facilitan la injerencia en el derecho fundamental a la protección de datos personales sin las debidas garantías (aps. 86), lo que se ve confirmado por el análisis de la Comisión acerca de la aplicación de los principios de puerto seguro (ap. 90). En palabras del Tribunal, "la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión [art. 7 de la Carta] exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario", considerando que "no se limita a lo estrictamente necesario una normativa que 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 a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización" (aps. 92 y 93). Además, destaca el Tribunal que "una normativa que no

prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta" (ap. 95).

En consecuencia, el Tribunal concluye que la Comisión no llevó a cabo una constatación debidamente motivada de que EEUU "garantiza efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión". Además, destaca la sentencia que el artículo 3.1 de la Decisión priva a las autoridades nacionales de las facultades de control previstas en la Directiva, lo que determina que la Decisión 2000/520/CE vulnere las exigencias del artículo 25.6 de la Directiva y deba ser declarada inválida.

Tras la sentencia *Schrems* se abre un incierto futuro, vinculado a las significativas diferencias entre los modelos de protección de datos prevalentes en EEUU y la UE, cuya coordinación se ve dificultada por las revelaciones relativas a las actividades de supervisión llevadas a cabo por las autoridades de EEUU. La inexistencia de un marco como el establecido en los principios de puerto seguro puede afectar de manera significativa a la prestación de muchos servicios, que cada vez más se basan en la computación en nube. Desde la perspectiva europea, resulta clave la concreta localización de dónde se produce el tratamiento de datos personales en los servicios de computación en nube, así como en el control de que las transferencias internacionales inherentes al funcionamiento de esos servicios no hacen posible el acceso a los datos por autoridades de terceros Estados sin las garantías adecuadas, como ha puesto de relieve nuevamente el Dictamen 02/2015 del llamado Grupo de Trabajo del artículo 29 ("Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing" de 22, de septiembre de 2015, pp. 6-8). En el nuevo contexto, a falta de un sistema que sustituya a los Principios de puerto seguro, se verá dificultada la prestación de tales servicios mediante el tratamiento de datos en EEUU.

Con respecto a las consecuencias inmediatas destaca la Declaración relativa a la aplicación de la sentencia *Schrems* adoptada el 16 de octubre por el llamado Grupo de Trabajo del artículo 29 que engloba a las autoridades nacionales de los Estados miembros (*http://ec.europa.eu/justice/data-protection/article-29/*), que incluye un llamamiento urgente para iniciar conversaciones con las autoridades de EEUU de cara a instaurar un nuevo mecanismo con garantías adecuadas. La Declaración pone de relieve que las transferencias que se lleven a cabo bajo el sistema de puerto seguro son ilegales tras la sentencia *Schrems*, mientras que las transferencias amparadas en cláusulas contractuales tipo y normas corporativas vinculantes (o BCRs) pueden seguir utilizándose, sin perjuicio de la eventual investigación de posibles reclamaciones por parte de las autoridades. En este marco, cobra especial importancia la interpretación de las excepciones previstas en el artículo 26.1 de la Directiva a la exigencia de autorización para la realización de transferencias, especialmente las relativas a la obtención del consentimiento inequívoco del interesado y a que la transferencia sea necesaria para la ejecución de un contrato entre interesado y responsable.

En todo caso, la sentencia *Schrems* debería representar un punto de inflexión que permita superar la situación tradicional en la que un marco muy estricto en materia de protección de datos ha ido unido a una aplicación muy deficiente también a las actividades en Europa de algunas de las principales entidades que se han beneficiado de los principios de puerto seguro, en perjuicio no sólo de los afectados sino también de las empresas de la UE cuya competitividad se ha visto menoscabada. Precisamente, es muy ilustrativa a este respecto la limitada (y muy tardía) efectividad de los controles de las autoridades nacionales en relación con la política de protección de datos de Facebook, red social a la que va referida el litigio principal. Esa deficiente aplicación se ve favorecida por el carácter gratuito -no sujeto al pago de una contraprestación monetaria- de muchos de los servicios que va unida a una menor exigencia por parte de los usuarios que no son conscientes del valor que tiene la información personal que de ellos se utiliza (también sin retribución económica).

III. Ley aplicable y autoridad competente en materia de protección de datos: la sentencia *Weltimmo*

1. Planteamiento

Tras la célebre sentencia *Google Spain* relativa al derecho al olvido, el asunto *Weltimmo* ha permitido de nuevo al Tribunal de Justicia abordar las complejas cuestiones que plantea en materia de determinación del Derecho aplicable el actual marco normativo de protección de datos de la UE. Dos aspectos, en concreto, son objeto de especial atención. Por una parte, como es sabido, a partir de lo dispuesto en el artículo 4.1.a) de la Directiva 95/46, la concreción de que el tratamiento de datos se efectúa en el marco de las actividades de un establecimiento del responsable en el territorio de un Estado miembro, resulta determinante de que el tratamiento quede sometido a la legislación europea, al tiempo que en el plano *ad intra* permite fijar la legislación nacional que resulta aplicable al tratamiento. Con respecto a este último aspecto, es clave la identificación del concreto Estado miembro en el que se considera que un responsable del tratamiento tiene el establecimiento en el marco del cual se efectúa el tratamiento en cuestión.

El asunto *Weltimmo* resulta especialmente de interés en aquellas situaciones en las que no cabe cuestionar que el responsable del tratamiento tiene un establecimiento en un Estado miembro pero realiza actividades en otro (u otros) Estado(s) miembro(s), en relación con las cuales puede surgir la duda de si el tratamiento se lleva a cabo en el marco de las actividades de un establecimiento del responsable en ese otro Estado miembro. En consecuencia, a estos efectos resulta de gran importancia cuándo cabe entender que un responsable tiene establecimientos en más de un Estado miembro, pues tal circunstancia es determinante para que pueda quedar sometido a las legislaciones (y eventualmente a sanciones por las autoridades de control) de más de un Estado miembro.

En concreto, el litigio principal en el asunto *Weltimmo* iba referido a una controversia entre la autoridad húngara de protección de datos y una empresa, con domicilio social en Eslovaquia, que gestiona una página web de intermediación

inmobiliaria en la que se anuncian inmuebles sitos en Hungría y algunos de cuyos anunciantes, residentes en Hungría habían presentado reclamaciones ante la autoridad húngara que pretendía sancionar a la empresa con domicilio social en Eslovaquia. Más allá de confirmar que el artículo 4.1.a) de la Directiva 95/46 excluye la posibilidad de que la autoridad húngara pueda aplicar la ley húngara a un responsable del tratamiento establecido exclusivamente en otro Estado miembro, la sentencia resulta relevante al fijar las pautas que pueden llevar a entender que el responsable del tratamiento tiene establecimientos en más de un Estado miembro y si el tratamiento en cuestión se ha realizado en el marco de un establecimiento situado en un Estado miembro distinto de aquel en el que tiene su domicilio social el responsable.

2. Determinación del establecimiento y ley aplicable

En virtud del artículo 4.1.a) Directiva 95/46 (traspuesto en nuestro ordenamiento en la LOPD y en su Reglamento):

«Los Estados miembros aplicarán las disposiciones nacionales que [hayan] 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».

Con respecto a la concreción de cuándo un responsable del tratamiento tiene un establecimiento en un Estado miembro (o potencialmente varios) distinto del Estado de su domicilio social, la sentencia, al igual que las conclusiones en dicho asunto del Abogado General Cruz Villalón presentadas el 25 de junio de 2015, establece, a partir del considerando 19 de la Directiva, que en materia de protección de datos se impone una concepción flexible de la noción de establecimiento, rechazando un enfoque formalista (y la idea de que una sociedad a estos efectos estaría establecida

exclusivamente en el Estado miembro en el que tenga su domicilio social). La existencia de un establecimiento en un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable. De hecho la sentencia (ap. 31) afirma que "el concepto de «establecimiento», en el sentido de la Directiva 95/46, se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable".

Como pone de relieve esta sentencia, para apreciar que se ejerce una actividad real y efectiva en un Estado miembro puede resultar determinante la gestión por parte de responsable de un sitio de Internet dirigido a dicho Estado (ap. 32). La nacionalidad de los afectados no se considera relevante a esos efectos. De acuerdo con su jurisprudencia previa –sentencias *Lindqvist* y *Google Spain*-, el Tribunal confirma que hacer referencia a datos personales en una página de Internet constituye un tratamiento de los mismos, que tiene lugar en el marco de las actividades que lleva a cabo quien gestiona el sitio de Internet en cuestión. Para apreciar que hay establecimiento, además del ejercicio efectivo y real de esa mínima actividad, es necesario la existencia de "una instalación estable" en el Estado en cuestión. La sentencia *Weltimmo* adopta un criterio según el cual debe valorarse "el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades… tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión", lo que en particular facilita la posibilidad de determinar que existe una instalación estable a esos efectos en un Estado distinto al del domicilio social especialmente para las empresas que se dedican a ofrecer servicios exclusivamente a través de Internet (ap. 29).

En concreto, puede bastar a tal fin la presencia en ese país de un único representante de la sociedad domiciliada en otro Estado "si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios concretos de los que se trate en el Estado miembro en cuestión" (ap. 30). Como circunstancias relevantes en el caso concreto para llevar a cabo esa apreciación, destaca el Tribunal: "se desprende que Weltimmo dispone de un representante en Hungría, que se menciona en el registro de sociedades eslovaco con una dirección en

Hungría y que intentó negociar con los anunciantes el pago de los créditos impagados. Dicho representante sirvió de enlace entre la citada sociedad y los denunciantes y la representó en los procedimientos administrativo y judicial. Por añadidura, la referida sociedad abrió una cuenta bancaria en Hungría, destinada al cobro de sus créditos, y utiliza un apartado de correos en el territorio de dicho Estado miembro para la gestión de sus asuntos corrientes". Se trata de factores que pueden resultar determinantes para apreciar en una situación como la controvertida en el asunto *Weltimmo*, la existencia de un «establecimiento», a efectos del artículo 4, apartado 1, letra a), de la Directiva 95/46. (ap. 33). Según los términos del propio fallo de la sentencia, para apreciar si existe establecimiento: "…el órgano jurisdiccional remitente puede tener en cuenta, 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."

En síntesis, para asegurar el elevado nivel de protección que persigue la Directiva, el enfoque adoptado por el Tribunal facilita la posibilidad de apreciar que a los efectos del artículo 4.1.a) de la Directiva 95/46 una sociedad puede considerarse establecida en Estados miembros distintos de aquel en el que tiene su domicilio social, lo que resulta determinante de que deba cumplir con la legislación sobre protección de datos (también) de ese otro Estado miembro y pueda ser sancionado por la autoridad de control de ese Estado en relación con el tratamiento de datos efectuado en el marco del establecimiento situado en su territorio.

3. Correlación entre ley aplicable y autoridad nacional competente

Cuando no quepa concluir que el responsable tiene un establecimiento en ese otro Estado miembro en el que también actúa, cobra importancia, la séptima cuestión

prejudicial planteada en el asunto *Weltimmo*, relativa básicamente a la interpretación del artículo 28.6 de la Directiva 95/46 y a las posibilidades de que la autoridad de control de un Estado miembro actúe incluso cuando conforme al artículo 4.1.a) sea aplicable el Derecho de otro Estado miembro. En virtud del mencionado artículo 28.6: "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." El apartado 3 del artículo 28 contempla, entre otros, poderes de investigación y de intervención.

El Tribunal destaca como punto de partida que el artículo 28.6 de la Directiva se vincula con la garantía de la libre circulación de los datos personales en la Unión, en particular para hacer posible la tutela de quienes se ven afectados por el tratamiento de datos personales llevado a cabo por quien estando sujeto al Derecho de un Estado miembro vulnera los derechos de personas en otro Estado miembro al que dirige su actividad pero en el que no está establecido (por carecer de cualquier instalación estable en ese otro Estado).

Para dar respuesta a esa séptima cuestión, el Tribunal de Justicia básicamente acoge la propuesta del Abogado General, que ofrecía un enfoque ponderado, coherente con el criterio básico de que –a diferencia de lo que sucede en el ámbito de las relaciones jurídico-privadas (piénsese, por ejemplo, en el caso de una eventual reclamación privada por daños derivados del incumplimiento de la legislación de protección de datos)- en relación con la aplicación jurídico-publica de la legislación sobre protección de datos, y en particular el ejercicio de la potestad sancionadora, el criterio de base es la correlación entre la legislación aplicable y la autoridad nacional competente. Ello resulta determinante de que la capacidad de actuación de la autoridad de control de un Estado miembro cuando resulte aplicable la ley sustantiva de otro Estado miembro, por estar establecido sólo allí el responsable del tratamiento, es limitada.

En los términos del apartado 57 de la sentencia: "…cuando una autoridad de control entienda de una denuncia, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, puede ejercer sus facultades de investigación sea cual sea el Derecho aplicable e incluso antes de saber cuál es el Derecho nacional aplicable al tratamiento de que se trata. Sin embargo, si llega a la conclusión de que es aplicable el Derecho de otro Estado miembro, no puede imponer sanciones fuera del territorio de su propio Estado miembro. En tal situación, le corresponde instar, en ejecución de la obligación de cooperación que se establece en el artículo 28, apartado 6, de la citada Directiva, a la autoridad de control de ese otro Estado miembro a declarar una eventual infracción de ese Derecho y a imponer sanciones si éste lo permite, basándose, en su caso, en la información que ella le haya remitido."

Ahora bien, es importante tener presente que estas consideraciones sólo son relevantes en la medida en que se concluya que el tratamiento no se efectúa en el marco de las actividades de un establecimiento del responsable en ese otro Estado miembro – a cuya autoridad de control se han dirigido los afectados-, y que, precisamente, el criterio al respecto adoptado por la sentencia, como se ha reseñado en el apartado anterior, facilita la posibilidad de apreciar a tales efectos que el responsable tiene su establecimiento en varios Estados miembros.

La próxima evolución de la legislación europea sobre protección de datos, mediante la aprobación del proyectado Reglamento en la materia a partir de la Propuesta de la Comisión de 2012 [COM(2012) 11 final] se contempla que altere sustancialmente la situación actual en relación estas cuestiones planteadas en el asunto *Weltimmo*. Precisamente la transformación en Reglamento y consiguiente unificación, privará en gran medida de relevancia a la cuestión de determinar la legislación de qué concreto Estado miembro resulta aplicable, en particular en el ámbito intracomunitario (no así en las situaciones vinculadas con terceros Estados). No debe extrañar que en tales circunstancias, la concreción de la autoridad nacional de control competente y el alcance de sus poderes hayan sido cuestiones especialmente controvertidas en el largo debate relativo a la aprobación del futuro reglamento.