



I

La presente consulta plantea si existe legitimación suficiente para el tratamiento de ciertos datos personales (se refiere en concreto al nombre de usuario y correo electrónico) de aquellos usuarios que denomina “ilegales”, que acceden a sus productos de software sin haber adquirido previamente los productos. En definitiva, la consultante pretende detectar el acceso ilegal a sus programas por parte de terceros no autorizados que no los hayan adquirido, sin haber cumplimentado el procedimiento de compra correspondiente. Plantea si cabe el uso de este software antipiratería sin el consentimiento del interesado, sobre la base del interés legítimo. Y si no se admitiera, plantea si cabe entender cumplido el deber de información y la obtención del consentimiento mediante la inclusión en la página web de la compañía de un aviso informativo sobre el tratamiento de datos personales en caso de acceso no autorizado. Finalmente, señala que los datos derivados de este sistema antipiratería serían transferidos a Estados Unidos, planteando si la transferencia internacional quedaría también amparada por el interés legítimo o si es necesaria la previa autorización.

Para estudiar las cuestiones planteadas en relación con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (en adelante, LOPD) y su normativa de desarrollo, debemos previamente estudiar **si existen datos personales** implicados, puesto que, de conformidad con el artículo 2.1 LOPD, *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*. Según el artículo 3.a) LOPD, se entiende por dato de carácter personal *“cualquier información concerniente a personas físicas identificadas o identificables”*; y en su desarrollo el artículo 5.1.g) del Real Decreto 1720/2007 de 21 de diciembre (en adelante, RDLOPD) define como dato de carácter personal *“cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”*. En este sentido, y a tenor del artículo 2.a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Y por tratamiento de datos el artículo 3.c) LOPD entiende *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y*

cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.

Según el escrito de consulta, el software antipiratería que pretende implantarse “podría implicar el acceso a datos de identificación como, por ejemplo, nombre, user name y correo electrónico del “usuario ilegal””. Por tanto, el propio escrito de consulta parte de la consideración de que se produciría el tratamiento de datos personales, tal y como ha venido considerando esta Agencia. Destacamos así el informe de 1 de marzo de 2007, que considera como dato de carácter personal el nombre de usuario como la dirección IP. En relación con esta última, la Sentencia de la Sección Primera de la Sala de lo Contencioso Administrativo de la Audiencia Nacional de 1 de septiembre de 2011, PO 625/2011, concluye también que la dirección IP tiene tal naturaleza. Señala así:

“Esta Sala desde sentencias antiguas como las dictadas en el recurso 132/2002 señaló que el concepto de dato personal es muy amplio y que el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de las personas, sino a cualquier tipo de dato personal, sea o no íntimo” añadiendo que la LO 15/1999 tiene por objeto garantizar y proteger, por lo que ahora interesa, los datos personales, entendiéndose por tales, ex art 3.a) de la citada Ley, “cualquier información concerniente a personas físicas identificadas o identificables”.

El criterio de la identificabilidad es básico para entender que la dirección IP debe ser considerada como dato personal y, por lo tanto, se encuentra sometida a las mismas garantías que resultan de lo previsto para cualquier clase de dato personal en relación a su tratamiento.

El Tribunal de Luxemburgo en el asunto C-275/2006 en relación, precisamente, a la cuestión planteada entre XXX e YYY ante el Juzgado de lo Mercantil numero 5 de Madrid, afirmó que: Tampoco se discute que la comunicación de los nombres y direcciones de determinados usuarios de ZZZ solicitada por XXX implique la comunicación de datos personales, es decir, de información sobre las personas físicas identificadas o identificables, conforme a la definición que figura en el artículo 2, letra a), de la Directiva 95/46 (véase, en este sentido, la sentencia de 6 de noviembre de 2003, Lindqvist, C-101/01, Rec. p. I-12971, apartado 24). Esta comunicación de datos que, según XXX, almacena YYY –cuestión que ésta no niega–, constituye un tratamiento de datos personales en el sentido del artículo 2, primer párrafo, de la Directiva 2002/58, en relación con el artículo 2, letra b), de la Directiva 95/46. En consecuencia, debe admitirse que dicha transmisión entra en el ámbito de aplicación de la Directiva 2002/58, observándose que la conformidad misma del almacenamiento de datos a los requisitos de esta Directiva no es objeto de discusión en el litigio principal.

También es importante para la cuestión que se plantea en este recurso el concepto de tratamiento de datos, para identificarlo con la actividad que realiza la recurrente y la empresa; el artículo 3.c) de la ley considera como tal operaciones y procedimientos técnicos de carácter automatizado o no, que



permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. El artículo 2.a/ de la Directiva 95/46/CE del Parlamento Europeo y del Consejo define el tratamiento de datos personales como "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación,...".

Como ya ha dicho esta Sala en multitud de ocasiones (Rec. 621/2004 ó 241/2005) no basta, sin embargo, la realización de una de estas actuaciones en relación con datos personales para que la ley despliegue sus efectos protectores y sus garantías y derechos del afectado. Es preciso algo más: que las actuaciones de recogida, grabación, conservación, etc.... se realicen de forma automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a un fichero.

Aplicando estos criterios, resulta que debemos concluir que lo que pretende la recurrente en relación a las direcciones IP de los usuarios de las redes P2P entra claramente en el concepto de tratamiento de datos y obligará, por lo tanto, a la aplicación de los criterios y exigencias generales del concepto de tratamiento de datos.

Sobre esta base normativa y de desarrollo, parece evidente que debemos concluir que la dirección IP es un dato personal e incluso que lo que pretende la parte recurrente es realizar un tratamiento de dichos datos que pretende llevar a efecto sin contar con el consentimiento del interesado. Al tratarse de datos personales y pretenderse efectuar un tratamiento, obviamente, debe aplicarse el artículo 5.5 de la LOPD al que ya nos hemos referido en el Fundamento jurídico Segundo de esta Sentencia, y cuyas circunstancias y exigencias, como hemos adelantado, no concurren".

También ha sido un criterio constante de esta Agencia el considerar el correo electrónico como dato de carácter personal, encuadrable en la definición genérica y en consecuencia mencionado entre los datos de carácter personal en el art. 2.2 RDLOPD. Así, destacamos los informes de 6 y 25 de octubre de 2004, afirmando el primero de ellos: "La dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, pudiendo incluso, en principio, coincidir con el nombre de otra persona distinta de la del titular.

De lo antedicho se desprende que podemos referirnos a dos supuestos esenciales de dirección de correo electrónico, atendiendo al grado de identificación que la misma realiza con el titular de la cuenta de correo:

El primero de ellos se refiere a aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado. En este supuesto, a nuestro juicio, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso dicha dirección ha de ser considerada como dato de carácter personal. Ejemplos característicos de este supuesto serían aquellos en los que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel con el propio del estado en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso delimitarse el centro de trabajo en que se realiza la prestación).

Un segundo supuesto sería aquel en que, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (por referirse, por ejemplo, el código de la cuenta de correo a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno). En este caso, un primer examen de este dato podría hacernos concluir que no nos encontramos ante un dato de carácter personal. Sin embargo, incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación. Por todo ello se considera que también en este caso, y en aras de asegurar, en los términos establecidos por la Jurisprudencia de nuestro Tribunal Constitucional, la máxima garantía de los Derechos Fundamentales de las personas, entre los que se encuentra el derecho a la "privacidad", consagrado por el artículo 18.4 de la Constitución, será necesario que la dirección de correo electrónico se encuentre amparada por el régimen establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Junto con estos dos supuestos, debe añadirse, evidentemente, que si en un fichero junto con la dirección de correo electrónico aparecieran otros datos que permitieran la identificación del sujeto (tales como su nombre y apellidos, su número de teléfono o su domicilio, conjunta o separadamente), la identificación sería absoluta y no se plantearía duda de que nos encontramos ante datos de carácter personal".

II

Así pues, no cabe duda de que el tratamiento que pretende realizarse afecta a datos personales de aquellos que acceden, sin la previa contratación del servicio, al software ofertado *on line* por la empresa consultante.

Partimos de la base, como lo hace la consulta, que resulta aplicable



territorialmente la legislación española sobre protección de datos personales. Nada se ha especificado en la consulta sobre este punto, pero parece darse a entender que el responsable del tratamiento (el que decida sobre la finalidad, contenido y uso del tratamiento, según el artículo 3.d) LOPD) se encuentra en alguno de los supuestos del artículo 2.1 LOPD y 3 del Reglamento de desarrollo, aprobado por Real Decreto 1720/2007 de 21 de diciembre (RDLOPD). Si no fuera así no tendrían sentido las cuestiones planteadas respecto a la legislación española.

Para que pueda existir un tratamiento de datos personales ha de existir una **legitimación** suficiente. El artículo 6 LOPD establece en sus dos primeros apartados las causas legitimadoras: *“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”*.

Es decir, con carácter general se requerirá el consentimiento del afectado, si bien no será necesario en los supuestos previstos en el apartado 2, sin que aparentemente nos encontremos ante ninguno de ellos, no existiendo relación comercial con los usuarios que acceden sin la previa contratación del servicio a los programas en cuestión.

Es por ello que la consultante plantea si el supuesto de hecho es subsumible en el interés legítimo al que se refiere el art. 7.f) de la Directiva 95/46/CE. Y es que, como es sabido, el artículo 6 LOPD supone la transposición al ordenamiento interno del mencionado art. 7 de la Directiva 95/46/CE de 24 de octubre de 1995 del Parlamento Europeo y del Consejo 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. Junto con otras causas legitimadoras, dispone el art. 7: *“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: (...) f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva”*.

El Tribunal Supremo, en el recurso 25/2008 de la Sección 6ª de la Sala 3ª, dirigido frente a determinados preceptos del RD 1720/2007, de 21 de diciembre, se cuestionó la adecuación o no al derecho comunitario del mencionado artículo 10.2.b) del RD 1720/2007, de 21 de diciembre, por lo que planteó una cuestión prejudicial al TJCE. Dicha cuestión prejudicial fue resuelta por el **Tribunal de Justicia de las Comunidades Europeas, en Sentencia de 24 de noviembre de 2011**, que contiene los siguientes pronunciamientos: “1. *Se opone al artículo 7.f) de la Directiva 95/46 la normativa nacional que, para permitir el tratamiento de datos, sin consentimiento, y necesario para la satisfacción de un interés legítimo (del responsable o del cesionario) exige que se respeten los derechos y libertades del interesado, y además que dichos datos figuren en fuentes accesibles al público, excluyendo de forma categórica y generalizada todo tratamiento que no figure en dichas fuentes.*

2. *El artículo 7.f) de la Directiva 95/46 tiene efecto directo”.*

Este pronunciamiento del Tribunal de Justicia se sustenta, entre otras, en las siguientes consideraciones:

El artículo 7, letra f) establece dos requisitos acumulativos para legitimar el tratamiento de datos:

Necesario para satisfacer un interés legítimo.

Que no prevalezcan derechos y libertades fundamentales del interesado. (Que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva).

El segundo requisito exige una ponderación de los derechos e intereses en conflicto que dependerá de las circunstancias concretas, teniendo en cuenta los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

A efectos de tal ponderación la lesión de los derechos fundamentales del afectado por el tratamiento puede variar en función de que los datos figuren ya, o no, en fuentes accesibles al público.

Los tratamientos que figuren en fuentes no accesibles al público implican necesariamente que el responsable o el cesionario del tratamiento dispondrán en lo sucesivo de cierta información sobre la vida privada del interesado. Lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta que debe ser apreciada en su justo valor, contrarrestándola con el interés legítimo del responsable o tercero.

Así pues, el artículo 7.f) de la Directiva 95/46/CE tiene efecto directo, siendo el interés legítimo presupuesto legitimador para el tratamiento de datos personales sin consentimiento del interesado, “*siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección”.*

Así pues, la **Sección 1ª de la Sala de lo Contencioso Administrativo de la Audiencia Nacional** viene realizando una ponderación caso por caso de la relación entre el interés legítimo y los derechos y libertades fundamentales del interesado. Así, la primera resolución que trató la cuestión fue la de **15 de marzo de 2012** dictada en el recurso 390/2010; respecto de la ponderación



señalaba que *“Ponderación de intereses en conflicto que dependerá de las circunstancias concretas de cada caso y en la que no obstante, sí puede tomarse en consideración, a efectos de determinar la posible lesión de los derechos fundamentales del afectado, el hecho de que los datos figuren ya, o no, en fuentes accesibles al público. Más ello, simplemente, como un elemento más de ponderación”*.

Y en ese caso concreto, relativo al tratamiento de datos relativos del libro genealógico de la cría de caballos de pura raza española, apreció que el interés legítimo del responsable del tratamiento debía prevalecer porque *“Nos hallamos, por tanto, ante unos datos personales extraídos de un sitio virtual, de acceso público, y que se exponen en la página web titularidad de la entidad actora (según resulta de las actuaciones) con la finalidad de dar información estadística sobre el caballo de pura raza española y posibilitar un rápido acceso a dicha información, sobretodo facilitar el cruce o comparación de datos entre todos los registros.*

Consideramos, por todo ello, que existen intereses legítimos de tal titular de la página web, e incluso intereses de terceros (de los propietarios o criadores de caballos) en acceder a dicha información publicada en Internet, intereses que se estiman prevalentes respecto del derecho a la protección de datos de los afectados por dicha información, y que por tanto excluyen la necesidad de consentimiento de los mismos”.

En parecido sentido la **Sentencia de 31 de mayo de 2012**, PO 793/2010, apreció el interés legítimo del miembro de un colegio oficial y una asociación para el tratamiento de datos de los integrantes del cuerpo electoral, puesto que se presentaba a las elecciones internas de dicho colegio oficial. Si bien en este supuesto existía también el consentimiento de los titulares de los datos personales.

La **Sentencia de 6 de junio de 2012**, PO 594/2009, apreció que el interés legítimo del responsable del fichero no debía prevalecer, en la ponderación, sobre la protección de datos personales, en los siguientes términos: *“La Sala, a la vista de las circunstancias concurrentes expuestas, considera que debe prevalecer el derecho a la protección de datos de los denunciados afectados incluidos en el citado fichero Domicilios, frente a los intereses particulares de la recurrente en explotar la citada base de datos que contiene nada menos que 37.000.000 de registros de datos personales, con la información asociada a los mismos ya indicada y recogida de la forma expuesta.*

En efecto, no es lo mismo que una determinada empresa necesite averiguar el domicilio de una persona de la que es acreedora, a efectos de poder efectuar el cobro de la deuda (para lo cual y a efectos de satisfacer ese interés legítimo puede utilizar los medios adecuados y lícitos tendentes a averiguar ese nuevo domicilio y poder tratarlo en orden a dicha finalidad), que

el hecho de la creación de un mega fichero como el que nos ocupa (que se reitera contiene 37.000.000 de registros de datos personales), con el fin de poder comercializarlo y ofrecer esa información obtenida. Además, como también se ha expuesto en algunos casos la información se asocia o abarca a las personas que conviven en el mismo domicilio que la que aparece registrada en el fichero, lo que conculca el derecho de protección de datos de los afectados

Por tanto, debe concluirse que no concurre el interés legítimo alegado por la entidad recurrente (que obviamente no es la persona física o jurídica que puede tener interés en el cobro de las posibles deudas) para tratar y, en correlación, ceder dichos datos de carácter personal, debiendo prevalecer el derecho de los afectados a la protección de datos, por lo que deben entenderse cometidas las infracciones apreciadas por la resolución impugnada”.

III

Expuesto el marco normativo y jurisprudencial sobre el interés legítimo del art. 7.f) de la Directiva 95/46/CE, procede estudiar si resultaría de aplicación al supuesto de hecho planteado.

Según el escrito de consulta, el interés legítimo invocado sería la protección de los programas informáticos suministrados por la empresa en cuestión, sus productos de software ofertados a los usuarios de la red. Se trata, por tanto, de un objeto de propiedad intelectual, de conformidad el artículo 10.1.i) del **Real Decreto Legislativo 1/1996, de 12 de abril por el que se aprueba la Ley de Propiedad Intelectual**. Y la ponderación deberá realizarse con la protección de los datos de carácter personal de aquellos que acceden a los programas de ordenador en cuestión sin haberlos adquirido en forma.

La propiedad intelectual aparece regulada en España en la Ley de Propiedad Intelectual indicada, y según el artículo 2 de dicha norma “*La propiedad intelectual está integrada por derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley*”. El contenido de la propiedad intelectual, constituido por derecho moral y patrimonial, es desarrollado en el Capítulo III del Título II de esta Ley; entre ellos, claro está, el derecho a la explotación de la obra, tal y como se pretende por la empresa consultante con el programa de ordenador correspondiente.

Sin embargo, la protección de la propiedad intelectual no es omnímoda: el artículo 40 ter señala que “*Lo dispuesto en los artículos del presente [Libro I](#), sobre la protección de las bases de datos, se entenderá sin perjuicio de cualesquiera otras disposiciones legales que afecten a la estructura o al contenido de cualesquiera de esas bases, tales como (...), protección de los datos de carácter personal*”. En el mismo sentido, el artículo 137 respecto del Título VIII del Libro II.

Además, este marco normativo debe completarse con la normativa



supranacional. Por un lado, el **Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio** (en lo sucesivo, “Acuerdo ADPIC”), que constituye el anexo 1 C del Acuerdo por el que se establece la Organización Mundial del Comercio (OMC), firmado en Marrakech el 15 de abril de 1994 - aplicable en España, al haber sido aprobado mediante la Decisión 94/800/CE del Consejo de la Unión Europea, de 22 de diciembre de 1994, relativa a la celebración en nombre de la Comunidad Europea, por lo que respecta a los temas de su competencia, de los acuerdos resultantes de las negociaciones multilaterales de la Ronda Uruguay (1986-1994).

Según el artículo 7, el objeto del Acuerdo ADPIC es el siguiente: *“La protección y la observancia de los derechos de propiedad intelectual deberán contribuir a la promoción de la innovación tecnológica y a la transferencia y difusión de la tecnología, en beneficio recíproco de los productores y de los usuarios de conocimientos tecnológicos y de modo que favorezcan el bienestar social y económico y el equilibrio de derechos y obligaciones”*. Y en consonancia la parte III versa sobre “Observancia de los derechos de propiedad intelectual” e instaura mecanismos de protección del derecho de propiedad intelectual, en el que se encuadran los programas de ordenador (art. 10).

En el marco del derecho comunitario, la Unión Europea ha realizado una importante armonización de las normas aplicables mediante Directivas europeas que obligan a los estados miembros a modificar sus normas nacionales. Se han aprobado así, directivas armonizando:

- la protección jurídica de los programas de ordenador: **Directiva 2009/24/CE** de 23 de abril sobre protección jurídica de programas de ordenador que impone a los Estados miembros proteger mediante derechos de autor los programas de ordenador.

- el plazo de duración de la protección de los derechos de autor: **Directiva 2006/116/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa al plazo de protección del derecho de autor y de determinados derechos afines**

- derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la Propiedad Intelectual: **Directiva 2006/115/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual.**

- el derecho de participación en beneficio del autor de una obra de arte original: **Directiva 2001/84/CE del Parlamento Europeo y del Consejo, de 27 de septiembre de 2001, relativa al derecho de participación en beneficio del autor de una obra de arte original**

- la protección jurídica de las bases de datos: **Directiva 96/9/CE** del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

- la protección jurídica de los servicios de acceso condicional o basados en dicho acceso: **Directiva 98/84/CE** del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso, que tiene por objeto proteger los servicios electrónicos de pago, incluyendo los servicios de la sociedad de la información que se presten a cambio de remuneración y sobre la base del acceso condicional, contra la piratería.

- derechos de autor y derechos afines a los derechos de autor en el ámbito de la radiodifusión vía satélite y de la distribución por cable: **Directiva 93/83/CEE** del Consejo, de 27 de septiembre de 1993, sobre coordinación de determinadas disposiciones relativas a los derechos de autor y derechos afines a los derechos de autor en el ámbito de la radiodifusión vía satélite y de la distribución por cable.

También tienen incidencia sobre la materia que nos ocupa la **Directiva 2000/31 de 8 de junio de 2000**, sobre Disposiciones relativas a la sociedad de la información y a la protección de la propiedad intelectual, en particular, de los derechos de autor tiene por objeto según el art. 1 *“contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros”*, si bien no se aplicará, según el art. 1.5.b) a *“a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE”*; es decir, a la protección de datos personales.

Asimismo, la **Directiva 2001/29 de 22 de mayo de 2001** sobre la protección jurídica de los derechos de autor y otros derechos afines a los derechos de autor en el mercado interior, con particular atención a la sociedad de la información. Finalmente, la **Directiva 2004/48 de 29 de abril de 2004** establece medidas, procedimientos y recursos necesarios para garantizar el respeto de los derechos de propiedad intelectual, si bien especifica el artículo 2.3 que *“La presente Directiva no afectará a: a) (...) la Directiva 95/46/CE”*.

Así, la normativa nacional y la comunitaria, junto con el Acuerdo ADPIC, instauran un marco de protección general de la propiedad intelectual, en el que se encuadran los programas de ordenador. Pero ya la regulación indicada prevé esta protección sin perjuicio de la debida a los datos de carácter personal.

Y es que el Tribunal de Justicia de las Comunidades Europeas ha tenido ya la oportunidad de ponderar la relación entre la protección a la propiedad intelectual y la protección de datos personales. Nos referimos a la **Sentencia dictada en Gran Sala de 29 de enero de 2008** dictada en la **cuestión prejudicial 275/2006** planteada por el Juzgado de lo Mercantil nº 5 de Madrid, en relación con la negativa de un prestador de servicios de comunicaciones a comunicar los datos personales de los usuarios a una entidad que actúa por cuenta de los titulares de derechos de propiedad intelectual agrupados en ella.



En particular, se pretendía que el prestador de servicios de comunicaciones electrónicas revelara la identidad y la dirección de determinadas personas a las que ésta presta un servicio de acceso a Internet y de las que se conoce su dirección IP y la fecha y hora de conexión, que habían utilizado un programa de intercambio de archivos peer to peer o P2P.

Así, tras estudiar la normativa comunitaria reguladora de la propiedad intelectual en relación con dicha cuestión, y considerar otros derechos fundamentales, como la tutela judicial efectiva, señalaba el apartado 63 que *“Sin embargo, es importante constatar que en la situación controvertida, respecto de la cual el órgano jurisdiccional remitente plantea esta cuestión, interviene, además de los dos derechos mencionados, otro derecho fundamental, a saber, el que garantiza la protección de los datos personales y, en consecuencia, de la intimidad”*.

Y pondera la relación entre la propiedad intelectual y la protección de los datos personales en los siguientes términos:

- “64 *Con arreglo al segundo considerando de la Directiva 2008/58, ésta pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta. En especial, pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de ésta. Dicho artículo 7 reproduce, en esencia, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950, que garantiza el respeto a la intimidad, y el artículo 8 de dicha Carta proclama expresamente el derecho a la protección de los datos personales.*
- 65 *De esta forma, la presente petición de decisión prejudicial plantea la cuestión de la necesaria conciliación de las exigencias relacionadas con la protección de distintos derechos fundamentales, a saber, por una parte, el derecho al respeto de la intimidad y, por otra parte, los derechos a la protección de la propiedad y a la tutela judicial efectiva.*
- 66 *Los mecanismos que permiten encontrar un justo equilibrio entre estos diferentes derechos e intereses se encuentran, por un lado, en la propia Directiva 2002/58, ya que establece normas que determinan en qué situaciones y en qué medida es lícito el tratamiento de datos personales y cuál es la tutela que debe dispensarse, y en las tres Directivas mencionadas por el órgano jurisdiccional remitente, que exceptúan el supuesto en que las medidas adoptadas para proteger los derechos que regulan afecten a la protección de los datos personales. Por otro lado, estos mecanismos deben resultar de la adopción, por parte de los Estados miembros, de disposiciones nacionales que garanticen la*

adaptación del Derecho interno a estas Directivas y de la aplicación de las citadas disposiciones por las autoridades nacionales (véase, en este sentido, en relación con la Directiva 95/46, la sentencia Lindqvist, antes citada, apartado 82).

- 67 *En cuanto a dichas Directivas, sus disposiciones tienen una naturaleza relativamente general, ya que deben aplicarse a un gran número de situaciones variadas que pueden presentarse en el conjunto de los Estados miembros. En consecuencia, contienen, lógicamente, normas que dejan a los Estados miembros un necesario margen de apreciación para definir medidas de adaptación del Derecho interno que puedan ajustarse a las diferentes situaciones previsibles (véase, en este sentido, la sentencia Lindqvist, antes citada, apartado 84).*
- 68 *Siendo esto así, corresponde a los Estados miembros, a la hora de adaptar su ordenamiento jurídico a las Directivas citadas, procurar basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico a estas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con dichas Directivas, sino también procurar que la interpretación de éstas que tomen como base no entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad (véanse, en este sentido, las sentencias Lindqvist, antes citada, apartado 87, y de 26 de junio de 2007, *Ordre des barreaux francophones et germanophone* y otros, C-305/05, Rec. p. I-0000, apartado 28).*
- 69 *Además, es preciso recordar, a este respecto, que el legislador comunitario ha exigido de forma explícita, a tenor de lo dispuesto en el artículo 15, apartado 1, de la Directiva 2002/58, que las medidas a que se refiere este apartado sean adoptadas por los Estados miembros de conformidad con los principios generales del Derecho comunitario, incluidos los mencionados en el artículo 6 UE, apartados 1 y 2.*
- 70 *A la vista del conjunto de las consideraciones anteriores, procede responder a la cuestión planteada que las Directivas 2000/31, 2001/29, 2004/48 y 2002/58 no obligan a los Estados miembros a imponer, en una situación como la del asunto principal, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. Sin embargo, el Derecho comunitario exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas,*



corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad”.

En definitiva, en la ponderación entre el interés legítimo del autor en proteger su obra – en este caso, un programa de ordenador – y la protección de datos de carácter personal se hace prevalecer la intimidad de las personas, considerando que las propias normas comunitarias y nacionales sobre propiedad intelectual prevén la salvaguarda de los datos de carácter personal; máxime cuando existen otros mecanismos para evitar accesos indebidos, y habiendo la legislación regulado importantes consecuencias en casos de piratería. En consecuencia, de los términos de la consulta podríamos inferir que no cabe la aplicación del artículo 7.f) de la Directiva 95/46/CE para la finalidad pretendida, debiendo la ponderación inclinarse hacia la protección de datos personales. Además, aunque se ha determinado la finalidad, tampoco se ha especificado cuál sería el destino concreto de los datos obtenidos por esta vía, ni el procedimiento de comunicación a las autoridades competentes.

IV

La consulta plantea, en segundo lugar, si no se admitiera el interés legítimo como fundamento suficiente para el tratamiento de los datos, si el consentimiento informado puede entenderse prestado *“mediante la inclusión en la Web Site de la Compañía de un aviso en el que se informará del tratamiento que se efectuaría de los datos personales en el caso de producirse accesos no autorizados a los productos de la Compañía y en el que expresamente se señalara que, en caso de acceder a estos productos de forma no autorizada, se consideraría que el usuario consiente al tratamiento señalado”.*

Se plantea, en definitiva, el modo de obtención del consentimiento a que se refiere el artículo 6.1 LOPD.

Debemos partir del artículo 2.h) de la Directiva 95/46/CE, que entiende por consentimiento del interesado *“toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan”.* En este mismo sentido, el artículo 3.h) de la Ley Orgánica 15/1999 de 13 de diciembre de protección de datos personales define el consentimiento del interesado como *“toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan”.*

Por tanto, el **consentimiento ha de ser previo** al tratamiento de datos personales; debe prestarse **libremente**, sin sometimiento a ningún tipo de

engaño, intimidación o coerción de ningún tipo; el consentimiento ha de ser **específico**, o concreto para determinada actividad y sólo para las finalidades concretas que hayan sido especificadas; **revocable** en cualquier momento; y en todo caso **inequívoco**. En este sentido, cabe una declaración de voluntad expresamente formulada, o bien implícitamente prestada, pero deberá en todo caso existir y acreditarse que existe tal consentimiento. Así, no entendemos suficiente que la genérica inclusión de la información en algún lugar de la página web suponga la obtención de un consentimiento inequívoco. No se especifica en qué modo se incluirían estos elementos en la página web, pero en este punto sería esencial - para entender debidamente cumplido el deber de información y la obtención del consentimiento - que se incorporen en la página web de tal modo que se asegure su lectura por el usuario. Todo ello para que no sea posible el uso del programa sin la previa lectura por el usuario. Será posible entender prestado el consentimiento siempre que, una vez ofrecida información suficiente, se advierta que en caso de seguir navegando en la página web en cuestión se entenderá que se consiente el tratamiento; pero para que el consentimiento sea previo e inequívoco, deberá implantarse algún medio técnico que asegure que la lectura de dicho apartado ha tenido lugar – como mediante una banda informativa estática en la parte superior de la página, una capa o DIV, una ventana desplegable, la marcación expresa de una casilla claramente visible y que no se encuentre ya marcada, o cualquier otro medio técnico que asegure su lectura, de forma que posteriormente pueda acreditarse la prestación del consentimiento. En este sentido, el artículo 6.1 no impone un procedimiento determinado para obtener el consentimiento, dejando libertad al responsable del fichero para establecer el que considere adecuado. Sin embargo, ha de tenerse en cuenta que el responsable del fichero será el que deba ofrecer prueba suficiente de la existencia del consentimiento. En este sentido, el artículo 12 del Reglamento con carácter general que *“Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.”*

Así, ya en el informe de 12 de mayo de 2011 indicábamos: *“Esta Agencia ha venido señalando, en cuanto al consentimiento informado se refiere, que éste habrá de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco tal y como exige la Ley”.*

Por último, el consentimiento ha de ser **informado**. El requisito de la información implica que el afectado conozca, con anterioridad al tratamiento, la existencia del mismo y las finalidades para las que se produce. Dispone el artículo 5.1 de la Ley Orgánica 15/1999 que *“Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

- a) *De la existencia de un fichero o tratamiento de datos de carácter*



personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.”

Respecto a la prueba del cumplimiento de dicho deber de información rige el principio de libertad de forma, de acuerdo con lo señalado en Sentencia del Tribunal Supremo de 15 de julio de 2010, en recurso contra el Real Decreto 1720/2007 que aprueba dicho Reglamento, por lo que podrá acreditarse por cualquier medio de prueba admisible en derecho. Pero deberá incluir, en todo caso, tal y como indica el artículo 12 RDLOPD, la delimitación del tratamiento o tratamientos concretos, la finalidad para los que se recaba así como las eventuales cesiones de datos con el contenido del art. 12.2 RDLOPD.

Finalmente, queremos destacar que la **transferencia internacional de datos** no quedaría amparada por el artículo 7.f) de la Directiva 95/46/CE, como se plantea en la consulta. Como ya hemos estudiado, el artículo 7.f) podría ser una causa legitimadora para el tratamiento de datos personales, como lo podría ser también el consentimiento del interesado cuyos datos se tratan. Es decir, son requisitos necesarios para poder tratar los datos personales. Una cosa es, por tanto, el presupuesto legitimador para el tratamiento, y otra muy distinta son las obligaciones que la legislación impone para el tratamiento, ya legitimado. Por ejemplo, incluso aunque el tratamiento esté suficientemente legitimado por alguno de los medios del artículo 7 de la Directiva 95/46/CE traspuesto por el artículo 6 LOPD, deberán cumplirse las obligaciones de inscripción del fichero en el Registro de esta Agencia (art. 26 LOPD), mantenimiento de la seguridad de los datos (art. 10 y Título VIII del Reglamento), atender el ejercicio de los derechos de acceso, rectificación, oposición y cancelación (arts. 15 y ss. LOPD). Y entre estas obligaciones de la normativa de protección de datos está la de obtener autorización previa del Director de esta Agencia cuando se realicen transferencias internacionales de datos con destino a países que no proporcionen un nivel de protección adecuado, de conformidad con los arts. 25 y ss. de la Directiva 95/46/CE, arts. 33 y 34 LOPD y Título VI del Reglamento 1720/2007. Por tanto, en caso de realizarse una transferencia internacional de datos habrán de cumplirse las obligaciones impuestas por dichos preceptos, sin que los mismos puedan quedar obviados por la vía del interés legítimo.

En este sentido, no sería precisa autorización del Director de la Agencia Española de Protección de Datos para el movimiento de datos dentro de los países del Espacio Económico Europeo (art. 5.1.s) RDLOPD), aunque deberá declararse la transferencia en el Registro General de Protección de Datos. De la misma manera, no sería necesaria autorización, aunque si debería efectuarse la correspondiente declaración al aludido Registro, en los casos en que la transferencia internacional tenga como destino un país que proporcione un nivel de protección equiparable al nuestro, siendo este último el caso en que se encuentran, entre otros, las entidades estadounidenses adheridas a los denominados “Principios de Puerto Seguro”. Por tanto, si la entidad a la que se transfieren los datos estuviera adherida a los principios de puerto seguro no será necesaria la autorización; y si no lo estuviera, deberá obtenerse dicha autorización previa.