



INFORME 0005/2016

La consulta plantea determinadas cuestiones derivadas de la relación entre la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) y la Disposición Adicional Novena de la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) añadida por la Disposición Final Segunda, apartado 16 de Ley 9/2014, de 9 de mayo de Telecomunicaciones.

En particular, plantea fundamentalmente tres cuestiones: i) si las direcciones IP son consideradas datos de carácter personal y la Disp. Ad. 9ª mencionada supone habilitación legal suficiente, a efectos del art. 11.2.a) LOPD, para las cesiones previstas en dicha disposición; ii) si por el contrario la mencionada disposición adicional está subordinada en su aplicación al desarrollo reglamentario; iii) y en caso afirmativo de la anterior, si cabe legitimar las cesiones de datos previstas en dicha disposición en el consentimiento de los usuarios, de conformidad con el art. 11.1 LOPD, manifestado en cláusulas contractuales y, en su caso, qué información debe proporcionarse a tales usuarios, especialmente en lo que atañe a la finalidad de la cesión.

I

Para un adecuado análisis de las cuestiones planteadas, comenzaremos examinando la **Disposición adicional novena LSSI**, que bajo la rúbrica “Gestión de incidentes de ciberseguridad que afecten a la red de Internet” dispone:

“1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o



servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio«. es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/ 2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley”.

En este sentido, hemos de destacar que ya el Apartado 20 de la **Directiva 2002/58/CE** del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) preveía la necesidad de adoptar medidas en relación con los riesgos de seguridad en una red abierta como Internet; focalizaba el tema en la adopción de medidas adecuadas por los proveedores de servicios para solucionar tales riesgos, así como informar a los usuarios de tales riesgos y las medidas a adoptar, - en relación con el art. 4 de dicha Directiva - en los siguientes términos:

“Los proveedores de servicios deben tomar las medidas adecuadas para salvaguardar la seguridad de sus servicios, de ser necesario en conjunción con el suministrador de la red, e informar a los abonados de todo riesgo especial relativo a la seguridad de la red. Tales riesgos pueden presentarse especialmente en el caso de los servicios de comunicaciones electrónicas a través de una red abierta como Internet o de una red de telefonía móvil analógica. Resulta particularmente importante que los abonados y usuarios de tales servicios sean plenamente informados por su proveedor de servicios de los riesgos para la seguridad que escapan a posibles soluciones adoptadas por dicho proveedor de servicios. Los proveedores de servicios que ofrecen servicios de comunicaciones electrónicas disponibles al público a través de Internet deben informar a usuarios y abonados de las medidas que pueden adoptar para proteger la seguridad de sus comunicaciones, por ejemplo utilizando determinados tipos de soporte lógico o tecnologías de cifrado. La



exigencia de informar a los abonados de riesgos de seguridad particulares no exime al proveedor del servicio de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para solucionar cualesquiera riesgos nuevos e imprevistos de seguridad y restablecer el nivel normal de seguridad del servicio. El suministro de información sobre riesgos de seguridad al abonado debe ser gratuito, salvo los costes nominales en que pueda incurrir el abonado al recibir o recoger la información, por ejemplo al cargar un mensaje de correo electrónico. La seguridad se valora a la luz del artículo 17 de la Directiva 95/46/CE”.

En estos términos son también esenciales las modificaciones introducidas en la Directiva 2002/58/CE por la **Directiva 2009/136/CE**; en particular destacamos los considerandos 57 a 61 así como el artículo 2, que modifica el art. 4 de la Directiva 2002/58 antes citado destacando la importancia de asegurar la seguridad de las redes y de la información, lo que supondrá un tratamiento de los datos de tráfico, con las consiguientes obligaciones del proveedor de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad, dando cuenta a las autoridades competentes y a los usuarios afectados de las violaciones que hayan tenido lugar. Destacamos especialmente la primera parte del considerando 58 de la Directiva 2009/136/CE que dispone: *“Las autoridades nacionales competentes deben promover los intereses de los ciudadanos, entre otras cosas contribuyendo a garantizar un nivel elevado de protección de los datos personales y de la intimidad. Con este fin, las autoridades nacionales competentes deben disponer de los medios necesarios para el ejercicio de sus funciones, incluidos datos completos y fidedignos sobre incidentes concretos de seguridad que hayan implicado un riesgo para los datos personales de los particulares”.*

Como es sabido, en España la trasposición de esta normativa comunitaria ha tenido lugar a través de la **Ley 9/2014 de Telecomunicaciones** ya citada. El Capítulo III del Título III de dicha norma desarrolla fundamentalmente estas cuestiones, complementado con las modificaciones introducidas en la LSSI cuyo estudio ahora abordamos.

II

La Disposición Adicional 9ª LSSI prevé la gestión de incidentes de seguridad que afecten a la red de Internet, y para ello establece un sistema de colaboraciones entre prestadores de servicios de la sociedad de la información, CERTs y autoridades competentes y órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad. En el marco de estas colaboraciones - cuyo fin esencial es resolver incidentes de seguridad, incluyendo la persecución de delitos, así como prevenir dichos incidentes - la norma en cuestión establece un intercambio de la información necesaria. Y como no podría ser de otro modo,



en el marco de este intercambio de información el apartado 2 incluye “*las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos*” [los incidentes de ciberseguridad].

Es por ello que la primera de las cuestiones planteadas por la consultante se refiere a la **naturaleza de la dirección IP**, para después cuestionar cuál es la legitimación para la cesión de dicho dato, si es que fuera dato de carácter personal.

Pues bien, tal y como indica la consulta, esta Agencia ha reiterado la consideración de la dirección IP como dato de carácter personal, sin que en la actualidad haya modificado su postura al respecto.

En este sentido se pronuncia el **Grupo de autoridades de protección de datos creado por el artículo 29 de la Directiva 95/46/CE en su Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007**, al señalar que:

“El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese sentido ha declarado que «los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva».

Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales.

Un caso particular sería el de algunos tipos de direcciones IP que en determinadas circunstancias y por diversas razones técnicas y organizativas no permiten realmente la identificación del usuario. Así sucede, por ejemplo, con las direcciones IP atribuidas a un ordenador instalado en un cibercafé, en el que no se pide identificación alguna a los clientes. En este caso, puede argüirse que los datos recogidos sobre el uso de un determinado ordenador «X» durante una determinada franja horaria no permiten la identificación del



usuario con medios razonables y, por lo tanto, no son datos personales. Sin embargo cabe señalar que, muy probablemente, los prestatarios de servicios de Internet no sabrán si la dirección IP en cuestión permite la identificación o no, y tratarán los datos asociados a ese IP de la misma manera que tratarían la información asociada a las direcciones IP de los usuarios debidamente registrados e identificables. Así pues, a menos que el prestatario de servicios de Internet sepa con absoluta certeza que los datos corresponden a usuarios que no pueden ser identificados, tendrá que tratar toda información IP como datos personales, para guardarse las espaldas.”

En este sentido, el considerando 26 de la Directiva 2002/58/CE y muy especialmente el considerando 52 de la Directiva 2009/136/CE, que indica que es conveniente *“seguir de cerca la evolución relacionada con el uso de las direcciones IP, teniendo en cuenta el trabajo realizado ya, entre otros, por el Grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos”*.

Y esta Agencia ha venido reiterando que el tratamiento y comunicación de las direcciones IP de los usuarios de Internet ha de ser considerado como un tratamiento de datos de carácter personal, sujeto a las disposiciones de la Ley Orgánica 15/1999, de conformidad con el art. 3.a) de dicha norma. Así, ya en el informe de 12 de septiembre de 2003 señalábamos:

“Para resolver la cuestión, debe partirse de la consideración de si una dirección de IP tiene el carácter de dato de carácter personal, dado que sólo en ese caso será aplicable al caso lo dispuesto en la Ley 15/1999, a tenor de lo establecido en su artículo 2.1.

Respecto a dicha cuestión, debe partirse en todo caso de la definición de dato de carácter personal que establece el artículo 3 a) de la Ley, que lo define como cualquier información concerniente a personas físicas identificadas o identificables.

El TCP/IP se trata de un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada una de los cuales contiene una dirección IP del emisor y del destinatario.

Por otro lado, el DNS (sistema de nombre de dominio) es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP.



Ciertas herramientas existentes en la red permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular.

A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.

En estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre dirección, número de teléfono, etc), por medios razonables, con lo que no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999.

En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas.

Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación.

Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos”.

Criterio reiterado en numerosas ocasiones, como en informes de 20 de julio de 2004, 11 de diciembre de 2006, 29 de abril y 15 de julio de 2008, 6 de agosto de 2010 y 30 de julio de 2014, entre otros muchos.



III

Si la dirección IP tiene la consideración de dato de carácter personal, hemos de plantearnos si cabe la **cesión o comunicación** de dicho dato, definida en el art. 3.i) LOPD como *“toda revelación de datos realizada a persona distinta del interesado”*. En este sentido, el art. 11 LOPD en su primer apartado prevé la cesión *“para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”*. Pero el apartado 2 del art. 11 exceptúa de la necesidad de consentimiento una serie de casos, entre ellos *“cuando la cesión esté autorizada en una ley”*. Esta Agencia ha venido reiteradamente señalando que en este artículo ha de interpretarse el término ley como Ley en sentido formal. Y así, la consultante plantea si la Disposición Adicional Novena LSSI constituye habilitación legal suficiente para amparar la cesión de las direcciones IP comprometidas o implicadas en el incidente de ciberseguridad.

La mencionada disposición adicional cumpliría con el requisito de ser ley en sentido formal, al aparecer contemplada en la Ley 34/2002. Sin embargo, si volvemos sobre ella concluimos que la previsión legal no está completa, al no definir quién será el cesionario de los datos personales y remitirse al desarrollo reglamentario para su completitud.

En este sentido, junto con los intercambios de información del párrafo segundo, el apartado 2 en su párrafo primero prevé el suministro *“de la información necesaria (...) para la adecuada gestión de los incidentes de ciberseguridad”*; es decir, prevé una cesión o comunicación así como la finalidad perseguida. También especifica el dato personal que será cedido, al indicar que incluirá *“las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos”*. Este apartado se refiere al cedente del dato, que serán *“los prestadores de servicios de la sociedad de la información”*; ahora bien este apartado 2.párrafo primero señala que el cesionario del dato será el *“CERT competente, y a las autoridades competentes”*.

La normativa no define qué es el CERT competente o autoridad competente. Únicamente el apartado j) del Anexo de la LSSI señala que por «Órgano competente» debe entenderse *“todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas”*. Y así se prevé en la propia norma, que asume que no existe aún tal definición para aplicar la Disposición estudiada, por cuanto el apartado 5 de se remite al desarrollo reglamentario – que aún no ha tenido lugar – para la determinación de *“los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente”*. Es decir, la



propia norma parte de la consideración de que uno de los parámetros subjetivos de la cesión, el cesionario, no está concretado en la norma, por lo que se remite al desarrollo reglamentario para ello.

En definitiva, la previsión legal que podría amparar la cesión pretendida no está completa, por cuanto aunque define el objeto de la cesión, su finalidad y el cedente, no se define al cesionario. Lo mismo sucede en los restantes apartados de la Disposición Adicional Novena, que tampoco determinan al cesionario a efectos de colaborar en la resolución de incidentes de ciberseguridad, incluyendo la persecución de delitos, ni en las fases de identificación de los usuarios afectados ni en el posible aislamiento de tales equipos o servicios.

Si tal previsión legal pudiera entenderse como completa, aunque fuera porque reglamentariamente se determinaran qué equipos de respuesta de incidentes pudieran considerarse competentes, podríamos entender que existe habilitación legal suficiente para la cesión. La previsión de la comunicación de datos estaría en una norma con rango de ley, aunque uno de sus parámetros subjetivos se delimitara reglamentariamente, pero ello podría no impedir la aplicabilidad del art. 11.2.a) LOPD. Ahora bien, mientras no exista determinación legal suficiente de todos y cada uno de los parámetros de la cesión no podemos entender que tal previsión legal existe.

En definitiva, si la ley habilitadora no prevé a quién se ceden los datos, no podemos entender que exista habilitación legal suficiente a los efectos del art. 11.2.a) LOPD.

Se responde también así a la segunda cuestión planteada en la consulta, por cuanto la ausencia del desarrollo reglamentario previsto en el apartado 5 sí supone un obstáculo, no a la cesión pretendida en sí misma, sino a la existencia de habilitación legal para la cesión.

Téngase en cuenta que en el borrador de Código de Buenas Prácticas para la gestión de incidentes de ciberseguridad elaborado por INCIBE que ha sido remitido junto con la consulta no se especifican los datos que serán objeto de cesión, pero ha de considerarse que es aplicable esta conclusión, especialmente a la vista de las recomendaciones 16 y 17, página 17 del mismo.

IV

A la vista de la conclusión anterior, cabe plantearse si existen otras causas que legitimen la cesión pretendida, en los términos del art. 11 LOPD. La consultante cuestiona si cabe obtener el consentimiento de los usuarios cuyas direcciones IP vayan a verse comprometidas o implicadas, a través de cláusulas específicas en los contratos de prestación de servicios. La respuesta debe ser afirmativa, por cuanto si se obtiene el consentimiento de los



afectados, que permitiera completar las previsiones de la disposición adicional novena (en el sentido de prever la cesión para las finalidades previstas, de los datos indicados y por parte del cedente, incluyendo específicamente quién sería el cesionario de los datos) cabría entender amparada la cesión en el art. 11.1 LOPD. Para ello debería ofrecerse información suficiente a los afectados en los términos del art. 5 LOPD, y en particular en cuanto a la finalidad de la cesión bastaría identificarla en los mismos términos que los previstos en la Disp. Ad. 9ª.

Ahora bien, cabe plantearse si tal consentimiento es necesario o si existirían otras causas que legítimamente ampararan la cesión pretendida. En particular, nos referimos al interés legítimo consagrado en el art. 7.f) de la Directiva 1995/46/CE, que considera lícito el tratamiento de datos de carácter personal si *“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 artículo 1 de la presente Directiva”*.

Esta Agencia ha tenido ya reiteradas ocasiones para analizar la incidencia que en el marco normativo de protección de datos ha ocasionado la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, pudiendo reproducir lo razonado por la misma en informe de 12 de marzo de 2012, referido a la creación de un fichero común para la colaboración entre entidades de un determinado sector en la prevención del blanqueo de capitales y la financiación del terrorismo. En el citado informe esta Agencia señalaba lo siguiente.

“(...) el marco normativo en materia de protección de datos se ha visto sensiblemente afectado por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en el seno de los recursos interpuestos por diversas asociaciones, entre ellas la propia consultante, contra el Reglamento de desarrollo de la Ley Orgánica 15/1999. A su vez, el marco se ve igualmente afectado por las Sentencias dictadas por el Tribunal Supremo en fecha 8 de febrero de 2012, por las que se resuelven los mencionados recursos.

La Sentencia del Tribunal de Justicia ha declarado expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) 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 artículo 1 de la presente Directiva”. Por ello, dicho



precepto deberá ser tomado directamente en cuenta en la aplicación de la normativa de protección de datos de carácter personal por los Estados Miembros, y en consecuencia por esta Agencia Española de Protección de Datos, dado que como señala el Tribunal Supremo en su sentencia de 8 de febrero de 2012 “produce efectos jurídicos inmediatos sin necesidad de normas nacionales para su aplicación, y que por ello puede hacerse valer ante las autoridades administrativas y judiciales cuando se observe su trasgresión”.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, el artículo 7 f) de la Directiva “*establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea 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, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado*” y, en relación con la citada ponderación, el apartado 40 recuerda que la misma “*dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado*”.

Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán “*procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión, por lo, conforme a su apartado 47 que “nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación*”.

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 de la Ley Orgánica 15/1999, según el cual “*la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*” o si, por el contrario, dichos derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar el tratamiento de los datos de carácter personal.



De este modo, esta Agencia ha venido analizando en los supuestos en los que así se ha planteado, si la ponderación de los derechos e intereses que concurren en cada caso concreto puede justificar o no el tratamiento de los datos de carácter personal, atendiendo a los criterios mencionados en la sentencia. En este punto, cabe igualmente señalar que el Tribunal de Justicia de la Unión Europea también ha tenido la ocasión de efectuar la mencionada ponderación en el supuesto analizado en la sentencia de 13 de mayo de 2014 (asunto Google).

En la ponderación mencionada esta Agencia Española de Protección de Datos ha venido poniendo de manifiesto que el establecimiento de garantías adicionales en relación con el tratamiento de los datos o la comunicación de los mismos que minoren el riesgo que sobre los afectados se deriva de los citados cesión o tratamiento puede ser tenido sustancialmente en consideración para admitir que la ponderación haya de efectuarse en favor del tratamiento o cesión.

De este modo, si las garantías adicionales permiten minimizar el perjuicio que puede producirse en los derechos e intereses de los afectados, y en particular en sus derechos a la intimidad y a la protección de datos de carácter personal, sería posible considerar lícito un tratamiento que, sin dichas garantías adicionales no podría considerarse fundado en un interés legítimo prevalente.

En el presente supuesto, en el que hemos concluido que mientras no se designen por la propia ley o por el desarrollo reglamentario los cesionarios de los datos no cabe entender que exista habilitación legal suficiente, nos planteamos si existe no obstante un interés legítimo en la cesión pretendida.

En primer lugar, existe un tratamiento de datos personales lícito, en el sentido que el tratamiento y la cesión de la dirección IP de los usuarios implicados o comprometidos en el incidente de ciberseguridad son necesarios para la satisfacción no sólo de un interés legítimo del que trata los datos, esto es, fundamentalmente el prestador de servicios de la sociedad de la información, ni siquiera sólo para el CERT competente y la autoridad competente, que perseguirán la resolución y prevención de los incidentes de ciberseguridad, sino para los usuarios afectados en particular y para el interés general de los ciudadanos con relación a la red de Internet. Uno de los obvios principios de todos los que actúen en la red, no sólo prestadores de servicios y autoridades competentes en sentido amplio sino cualquier usuario, es la preservación de la seguridad de las redes y de la información.

Debemos aquí traer a colación toda la normativa, tanto comunitaria como estatal, indicada en el apartado I del presente informe, que si prevé la adopción de medidas técnicas y organizativas necesarias para garantizar la



seguridad, tanto directamente por los proveedores de servicios como la información a los usuarios y a las autoridades competentes de las violaciones de seguridad, es precisamente porque a todos interesa el mantenimiento de las redes en un adecuado estado de seguridad, lo que implicará la lucha contra las ciberamenazas y ciberataques. Destacamos de nuevo el considerando 57 de la Directiva 2009/136/CE, que se centra en la adopción de estas medidas por el proveedor de un servicio de comunicaciones electrónicas disponible al público, así como en el establecimiento de *“una política de seguridad para el tratamiento de los datos personales, a fin de identificar las vulnerabilidades del sistema, y proceder, de manera periódica, a una supervisión y a la adopción de medidas preventivas, correctoras y paliativas”*.

La ciberseguridad no sólo interesa, como es lógico, a los prestadores de servicios de la sociedad de la información, sino a toda la colectividad usuaria de las redes y por ello a las autoridades competentes designadas para velar por esta seguridad. Así, el considerando 58 de la misma Directiva prevé, sin perjuicio de una adecuada protección de los datos personales, una cesión de los datos necesarios para prevenir y gestionar los incidentes concretos de seguridad: *“Las autoridades nacionales competentes deben promover los intereses de los ciudadanos, entre otras cosas contribuyendo a garantizar un nivel elevado de protección de los datos personales y de la intimidad. Con este fin, las autoridades nacionales competentes deben disponer de los medios necesarios para el ejercicio de sus funciones, incluidos datos completos y fidedignos sobre incidentes concretos de seguridad que hayan implicado un riesgo para los datos personales de los particulares. Deben supervisar las medidas adoptadas y difundir las mejores prácticas entre los proveedores de servicios de comunicaciones electrónicas disponibles al público. Los proveedores deben llevar por tanto un inventario de las violaciones de los datos personales que permita el análisis y la evaluación posteriores por parte de las autoridades nacionales competentes”*. Aunque la notificación de las violaciones de seguridad, en los términos de la Ley de Telecomunicaciones, en particular su artículo 41, sea realizada a esta Agencia Española de Protección de Datos, ello no impide que de conformidad con el art. 44 de la misma norma la preservación de la integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas conlleve, para la necesaria gestión y prevención de los incidentes, el tratamiento y cesión de los datos personales en cuestión.

Y más aún, la ciberseguridad reiteramos que no sólo interesa a los prestadores de servicios, y a las autoridades competentes, sino que la misma Directiva prevé que tiene por objeto esencial proteger a los abonados o particulares afectados, motivo por el cual la normativa comunitaria e interna prevén las correspondientes notificaciones. Su fundamento se detalla en el considerando 61 de la Directiva 2009/136/CE, que destaca que *“una violación de los datos personales puede causar, si no se toman medidas de manera rápida y adecuada, pérdidas económicas sustanciales y perjuicios sociales para el abonado o particular afectado, incluida la usurpación de la identidad”* y



por ello prevé una notificación inmediata a los afectados y a la autoridad competente, detallando cuándo debe considerarse que *“una violación afecta negativamente a los datos y la intimidad del abonado o particular”*.

Más aún, la Directiva contempla que preservar la seguridad sirve del interés general de los ciudadanos. Destacamos especialmente el considerando 59, en su segundo inciso: *“No obstante, la notificación de violaciones de la seguridad refleja un interés general de los ciudadanos por ser informados acerca de fallos en la seguridad que puedan implicar la pérdida de sus datos personales o algún otro riesgo para dichos datos, y acerca de las precauciones disponibles o aconsejables que pueden tomar para minimizar las posibles pérdidas económicas o el daño social resultantes de dichas violaciones. Este interés de los usuarios por ser informados no se limita, obviamente, al sector de las comunicaciones electrónicas, por lo que deben introducirse, a escala comunitaria y con carácter prioritario, requisitos de notificación explícitos y obligatorios en todos los sectores. A la espera de una revisión por la Comisión de toda la legislación comunitaria en ese ámbito, la Comisión debe, en consulta con el Supervisor Europeo de Protección de Datos, adoptar inmediatamente las medidas adecuadas para fomentar la aplicación en toda la Comunidad de los principios contenidos en las normas sobre notificación de violaciones de datos recogidas en la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), independientemente del sector o del tipo de datos en cuestión”*.

El segundo parámetro del interés legítimo exige que no prevalezcan los derechos y libertades fundamentales del interesado, en este caso el derecho a la protección de sus datos personales, que serían objeto de cesión en los incidentes de ciberseguridad.

Y entendemos de en este segundo criterio de ponderación también la normativa, tanto comunitaria como estatal, estudiada ha realizado indudablemente una ponderación a favor de la cesión pretendida.

Específicamente, el considerando 57 de la Directiva 2009/136/CE ya prevé un posible equilibrio entre la normativa sobre protección de datos personales y las medidas que persiguen la ciberseguridad, al establecer que *“Sin perjuicio de la Directiva 95/46/CE, dichas medidas deben velar por que únicamente pueda acceder a los datos personales el personal debidamente autorizado para fines legales, así como por la protección de los datos personales almacenados o transmitidos y de las redes y los servicios”*.

Y aún más específicamente el considerando 53 prevé el tratamiento de datos de tráfico por parte de los proveedores de servicios al amparo del art. 7.f) de la Directiva, criterio que puede extenderse a la comunicación de tales datos a los equipos a los que corresponda la respuesta a los incidentes de seguridad y, con mayor legitimidad aún, a las autoridades competentes. Afirma el



mencionado considerando: *“El tratamiento de los datos de tráfico en la medida estrictamente necesaria para asegurar la seguridad de las redes y de la información, es decir, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y la seguridad de los servicios conexos que dichas redes y sistemas ofrecen o hacen accesibles, por parte de los proveedores de tecnologías y servicios de seguridad cuando actúen como responsables del tratamiento de los datos, queda sujeto al artículo 7, letra f), de la Directiva 95/46/CE. Esto puede, por ejemplo, incluir el evitar el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución de códigos maliciosos, y el poner fin a los ataques de «denegación de servicio» y los daños a los sistemas informáticos y de comunicación electrónica”.*

Para esta ponderación se han considerado todos los parámetros utilizados en la propia Disposición Adicional Novena LSSI estudiada. En primer lugar, la finalidad de la cesión configurada como la gestión de incidentes de ciberseguridad que afecten a la red de internet, planteado en un sentido amplio; esto es, tanto para la prevención debida como para la gestión de los incidentes que surjan. Y sólo en este segundo campo las recomendaciones del código de buenas prácticas plantean el intercambio de información. En segundo lugar, el objeto de la cesión se deberá limitar a la información estrictamente necesaria para la adecuada gestión de tales incidentes. Como antes decíamos, el código de buenas prácticas no detalla el objeto de la información, pero la consulta se ha ceñido a la cuestión de la dirección IP, dato de carácter personal cuya comunicación será estrictamente necesaria para la gestión de tales incidentes, tal y como prevé la disposición estudiada.

Y en tercer lugar, volvemos a la consideración de cedente y cesionario de los datos en cuestión, pero ahora estudiado desde el punto de vista de la ponderación. En cuanto al cedente, lo serán los prestadores de servicios de la sociedad de la información, que serán los que puedan disponer de las direcciones IP que puedan estar comprometidas o implicadas en el incidente en concreto.

Y en esta ponderación también ha sido esencial considerar el cesionario propuesto por la consultante, completando así el parámetro que faltaba por determinar en la Disp. Ad. 9ª; esto es, que la consultante no plantea un sistema general de comunicación a cualquier tipo de CERT, sino que presenta un código de buenas prácticas para la gestión de incidentes de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), antiguo INTECO, que es una sociedad pública estatal cuyo capital corresponde a Red.es, que a su vez es una entidad pública empresarial adscrita al Ministerio de Industria, Energía y Turismo. El hecho de que el parámetro subjetivo cuya falta de determinación en la Disposición Adicional Novena LSSI (el cesionario de los datos) se complete



con la identificación de una sociedad de capital íntegramente público, adscrita a una entidad pública empresarial, y no a una entidad de base privada supone una salvaguardia más a la necesaria protección de los datos personales de los usuarios. Especialmente en este punto hemos considerado que de conformidad con el código de buenas prácticas aportado, las actuaciones se enmarcan en la Estrategia de Seguridad Nacional, en la Estrategia Europea de Ciberseguridad y dentro de la Agenda Digital para España en el Plan de Confianza en el Ámbito Digital. El punto neutro de gestión de incidentes será así operado por INCIBE. Y en definitiva el mencionado código se configura *“como paso previo y facilitador en la adopción de futuras exigencias normativas que deberán ser implementadas por los PSSI en nuestro país en un corto plazo de tiempo (una vez aprobada la Directiva NIS y el desarrollo de la Disposición Adicional Novena de la LSSI)”*. El carácter público, en un sentido amplio, de la sociedad pública estatal seleccionada, unido a la justificación en las estrategias nacionales y europeas y su consideración de paso previo a un sistema basado en nueva normativa son parámetros esenciales en orden a ponderar el sistema en cuestión a favor del interés legítimo de la cesión pretendida.

En **conclusión**, la consideración de la dirección IP como dato de carácter personal determina que la comunicación de la misma por los prestadores de servicios de la sociedad de la información al CERT competente haya de estar amparada en alguna de las causas del art. 11 LOPD. A estos efectos, no se considera habilitación legal suficiente la Disposición Adicional Novena LSSI por no determinar el cesionario de los datos, al limitarse a señalar a los CERT competentes que habrán de ser determinados en el desarrollo reglamentario. Sin perjuicio de poder amparar la cesión en el consentimiento de los afectados, cabe entender que, con las salvaguardias señaladas en el apartado III del presente informe para realizar la ponderación, la comunicación de la dirección IP queda amparada por el interés legítimo del art. 7.f) de la Directiva 1995/46/CE.