Cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad. Informe 213/2004

Cesión del dato de la dirección IP a las Fuerzas y Cuerpos de Seguridad

La consulta plantea si la entidad consultante puede “comunicar a las Fuerzas y Cuerpos de Seguridad del Estado datos de dirección IP, fecha y hora de conexión de un usuario previo consentimiento ni mandamiento judicial” cuando la propia entidad presente una denuncia.

Como cuestión previa, debe indicarse que el presente informe se limitará a analizar la cuestión planteada desde el punto de vista de la aplicación al supuesto planteado de las normas reguladoras del derecho fundamental a la protección de datos de carácter personal, contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y sus disposiciones de desarrollo, sin entrar a valorar si dicha conducta incide en cualquier otro derecho de los usuarios, al no ser dicho análisis competencia de esta Agencia Española de Protección de Datos.

Sentado lo anterior, la primera cuestión que debe plantearse en el presente caso es la de si la dirección IP de un usuario de Internet constituye un dato de carácter personal.

La cuestión fue detenidamente analizada en nuestro informe de 12 de septiembre de 2003, en el que se señalaba lo siguiente:

“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 mas, 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.”

En el presente caso, además, debe tenerse en cuenta que, según se indica en la consulta, la comunicación del dato de la dirección IP se efectúa en el ámbito

de una determinada denuncia, por lo que o bien se facilitará, en caso de conocerse inequívocamente, el dato del usuario asociado a la misma o bien la comunicación tendrá por objeto, precisamente, la averiguación del sujeto autor de los hechos denunciados, por lo que ha de concluirse que los datos a los que se refiere la consulta se encuentran sometidos a las previsiones de la Ley Orgánica 15/1999.

Resultando, en consecuencia, de aplicación lo dispuesto en la Ley Orgánica 15/1999, la transmisión de los datos mencionados en la consulta a las Fuerzas y Cuerpos de Seguridad constituirá una cesión o comunicación de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica como “Toda revelación de datos realizada a una persona distinta del interesado”.

En caso de cesión de datos, el artículo 11.1 de la Ley Orgánica 15/1999 dispone que “Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”. No obstante, será lícita la comunicación de datos sin consentimiento del interesado, como sucedería en el supuesto contemplado en el presente caso, si la misma encuentra encaje en los casos mencionados en el artículo 11.2 de la Ley, considerando el apartado a) de dicho precepto lícita la cesión habilitada por una norma con rango de Ley.

En el presente caso, la consulta se refiere a la presentación de una denuncia ante las Fuerzas y Cuerpos de Seguridad, siendo preciso recordar que, en este sentido, el artículo 259 de la Ley de Enjuiciamiento Criminal dispone que “el que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal, o funcionario fiscal más próximo al sitio en que se hallare”, añadiendo el artículo 262 que “los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio Fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante”.

Por otra parte, el artículo 12.1 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico dispone que “Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce

meses, en los términos establecidos en este artículo y en su normativa de desarrollo".

Añade, a su vez, el artículo 12.3 de la propia Ley 34/2002 que "Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales", señalando el último párrafo del artículo 12.2 que "Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos".

Como se ha indicado, la comunicación de los datos a las Fuerzas y Cuerpos de Seguridad deberá someterse a lo establecido en la Ley Orgánica 15/1999, cuyo artículo 22.2 dispone que "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad".

Esta Agencia Española de Protección de Datos ha venido considerando que el tratamiento de datos por parte de las Fuerzas y Cuerpos de Seguridad al amparo de lo dispuesto en el artículo 22.2 citado será posible siempre y cuando se cumplan los siguientes requisitos, enumerados en informe de 16 de julio de 1999:

a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.

b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.

c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.

d) Que, en cumplimiento del artículo 20.4 de la LORTAD, los datos sean cancelados “cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento”.

En el presente caso, descartando los apartados b) y c) anteriormente citados, al tratarse no de una solicitud de información efectuada por las Fuerzas y Cuerpos de Seguridad, sino de los datos necesarios para la presentación de una denuncia, tal y como se indica en la consulta, ante dichas Fuerzas y Cuerpos, la cesión de dichos datos se encontrará amparada en caso de que la denuncia se presente por la concurrencia de un peligro real y grave para la seguridad pública o existan indicios fundados en el denunciante para considerar que se han producido unos hechos constitutivos de una infracción penal que ha de ser objeto de persecución por parte de las Fuerzas y Cuerpos de Seguridad.

De este modo, siempre que se den esos indicios razonables habría que considerar que el tratamiento de los datos cedidos por parte de las Fuerzas y Cuerpos de Seguridad será conforme a lo exigido por la Ley Orgánica 15/1999, siendo en consecuencia conforme a la misma la cesión de los datos por parte de la consultante.

A la vista de lo que se ha venido indicando, y teniendo en cuenta exclusivamente la incidencia en el supuesto planteado de lo dispuesto en la Ley Orgánica 15/1999, debe considerarse que la cesión de los datos se encontraría amparada en lo previsto en el artículo 11.2 a) de la misma, en conexión con las normas de la Ley de Enjuiciamiento Criminal que se han citado en el presente informe, así como en el artículo 22.2 de la Ley Orgánica 15/1999 en relación con el artículo 12.3 de la Ley 34/2002.