AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Informe 0482/2011

I

La consulta plantea la conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y en su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, del procedimiento de monitorización del tránsito de mensajes SMS que circulan por la red de la consultante para identificar aquéllos que supongan una suplantación de identidad en las comunicaciones remitidas por las entidades bancarias a sus clientes, determinando en que supuestos se ha podido producir una simulación de la identidad de la entidad.

Según se describe en la consulta el procedimiento implicaría la existencia de una serie de fases sucesivas que implicarían asimismo sucesivos tratamientos de datos, debiendo en cada caso determinarse el alcance y legitimación para el tratamiento de tales informaciones a la luz de lo dispuesto en la Ley Orgánica 15/1999. De este modo:

En una primera fase, las entidades facilitarían a la consultante los datos identificativos de los centros servidores de SMS desde los cuales aquéllas remitirían habitualmente los citados mensajes a sus clientes.

En la segunda fase, la consultante rastrearía los mensajes remitidos en que constase la cabecera de la entidad financiera, contrastando para los mismos la procedencia del mensaje. De este modo, si la cabecera procediera de uno de los centros servidores no existiría problema alguno, verificándose, por su parte, aquellos casos en los que el mensaje no procediera del centro servidor declarado por la entidad.

En un tercer momento, y en relación exclusivamente con aquellos supuestos en que los mensajes no aparezcan como enviados desde un centro servidor utilizado por la entidad financiera, la consultante aplicaría sobre los números destinatarios de los mensajes una función HASH, remitiendo el dato resultante de dicha función a la entidad financiera. La misma función será facilitada a la entidad a fin de que por la misma pueda conocerse qué números telefónicos de entre los de sus clientes han podido ser objeto de la suplantación, pudiendo en ese caso adoptar las medidas que estime necesarias para prevenir el fraude que pudiera haberse llevado a cabo.

II

En la consulta se señalan una serie de especificaciones que resultan igualmente relevantes para comprender el procedimiento descrito:

Así, por una parte, se indica que la función HASH “podría asociarse a varios números de teléfono”, pudiendo algunos de ellos coincidir con los de los clientes de la entidad y otros no.

Del mismo modo, de la afirmación que acaba de reproducirse parece desprenderse que es posible que la función haya sido facilitada por la consultante a la entidad bancaria habiéndola obtenido de un determinado número de teléfono que no se corresponda con ningún cliente de la entidad o viceversa; es decir, al no identificar un único número de teléfono, no existe una relación unívoca entre la función y los números que respondan a la misma.

Dado que la entidad financiera podría eventualmente acceder a número de teléfono de terceros no clientes de la entidad si aplicase la función HASH a todo el rango de numeración, la consulta incluye, por último una serie de cautelas, denominadas “medidas de seguridad”, tendentes a evitar un mal uso de la herramienta contratada. Dichas garantías implican:

- Por una parte, la modificación mensual de la función, a fin de que no sea posible la realización de tratamientos históricos con la finalidad de obtener más información que la requerida para la lucha contra el fraude que implicaría la suplantación detectada.

- Por otra, la exigencia contractual de que la entidad que contrate el servicio se abstenga de aplicar la función HASH sobre números telefónicos distintos de los de sus clientes.

- En tercer lugar, la exigencia contractual de que se informe por parte de la entidad a sus clientes acerca del tratamiento necesario de su número telefónico a fin de evitar la suplantación.

- Finalmente, la reserva a favor de la consultante de la posibilidad de verificar el cumplimiento por las entidades de los dos puntos anteriormente señalados, así como de la facultad resolver el contrato en caso de incumplimiento.

III

Como se ha indicado, el sistema implica operaciones sucesivas que serán realizadas con la información necesaria para llevar a cabo el análisis

descrito: en primer lugar se producirá una transmisión de la información desde las entidades bancarias a la consultante; en segundo lugar, la propia consultante procederá a un tratamiento de la información, analizando la coincidencia de la cabecera del mensaje y de su remitente y aplicando en caso de no producirse dicha coincidencia la función HASH a la que se ha hecho referencia; la tercera implicará la transmisión por la consultante a las entidades de la información resultante de la aplicación de la citada función; y finalmente la propia entidad verificará la correspondencia de la función con los datos de sus clientes, adoptando las medidas que procedan. Será necesario comprobar si todos estos supuestos implican el tratamiento de datos de carácter personal y si los mismos se encuentran legitimados conforme a lo previsto en la Ley Orgánica 15/1999 y su Reglamento de desarrollo.

Como cuestión previa, es preciso señalar, como acaba de indicarse, si en todos los supuestos planteados estamos o no es presencia de datos de carácter personal. A tal efecto, el artículo 5.1 f) del Reglamento de desarrollo de la Ley Orgánica 15/1999 define como datos de carácter personal “Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”, siendo según el artículo 5.1 o) persona identificable “toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados”.

Por su parte, el artículo 5.1 e) del Reglamento define dato disociado como “aquél que no permite la identificación de un afectado o interesado”; es decir, el dato habrá sido sometido a un previo procedimiento de disociación, definido por el artículo 5.1 o) como “todo tratamiento de datos personales que permita la obtención de datos disociados”.

La primera de las definiciones a la que se ha hecho referencia resulta especialmente relevante en relación con la determinación de la naturaleza de la información referida a los centros servidores de las entidades financieras que se adhieran al sistema descrito en la consulta, por cuanto tal información vendrá, según se indica en la consulta, asociadas a la propia entidad financiera. En consecuencia, los datos identificativos de los centros servidores de datos vendrán asociadas a la entidad financiera o dichas terceras entidades, pero no a una persona física, lo que excluiría la aplicación a estos datos de la normativa reguladora del derecho fundamental a la protección de datos de carácter personal.

Las definiciones relacionadas con la identificabilidad o no del afectado y

con el hecho de que los datos hayan sido previamente sometidos a un procedimiento de disociación deben ser analizadas en relación con la información facilitada por la consultante a las entidades, consistente en la aplicación de una función HASH sobre los datos correspondientes a los números telefónicos destinatarios de los SMS respecto de los que existiera un indicio de suplantación al no corresponderse el dato del remitente con la identificación de los centros servidores facilitados por la entidad de crédito.

En relación con este punto, esta Agencia viene reiterando en numerosos informes (por todos ellos el de 13 de julio de 2011) que “para que un procedimiento de disociación pueda ser considerado suficiente a los efectos de la Ley Orgánica 15/1999, será necesario que de la aplicación de dicho procedimiento resulte imposible asociar los datos a un sujeto determinado. En este sentido, las disposiciones internacionales reguladoras de la protección de datos de carácter personal vienen a considerar que el afectado no será determinable cuando su identificación exija un esfuerzo desproporcionado que sea suficiente para disuadir a quien accede al dato de la identificación de la persona a la que el mismo se refiere”.

Pues bien, en el supuesto planteado en la consulta, se señala por la consultante que la misma “nunca facilita los números de teléfono en claro” y que la función HASH “podría asociarse a varios números de teléfono”, de forma que “sólo cuando dicho número/código coincida con el número de teléfono de un cliente, el banco podrá descifrar el HASH”.

En resumidas cuentas, de lo señalado en la consulta se desprende que la información facilitada por la consultante identifica diversos números telefónicos, pudiendo algunos de ellos coincidir con los de clientes de la entidad y otros no; es decir, no existe una identificación unívoca de un número telefónico individualizado con el resultado de la aplicación de la función facilitada por la consultante, sino que dicha función será asociable con una pluralidad de números, no pudiendo la entidad receptora de la información conocer si la suplantación se ha producido respecto de uno o varios de ellos o si efectivamente se ha producido dicha suplantación mediante la remisión del mensaje a un cliente del banco o a otra persona distinta pero respecto de la que el resultado de la aplicación del algoritmo en que consiste la función HASH sea coincidente.

De este modo, sólo en caso de conocerse el dato del número telefónico, lo que en principio sólo sucedería respecto de los clientes de la entidad financiera, sería posible revertir la función e identificar el número telefónico, mientras que respecto de los restantes números a los que sea aplicable la función no sería posible revertir dicha función para determinar el número telefónico. Del mismo modo, si ninguno de los números asociados a un determinado resultado de la aplicación de la función se correspondiese con los clientes de la entidad, dicha entidad no conocería quiénes son los destinatarios

de los mensajes respecto de los que se produce la suplantación.

A fin de garantizar que esa circunstancia concurra efectivamente en la práctica, la consulta aclara que en los contratos celebrados con las entidades se especificará terminantemente que las mismas se comprometen a no aplicar la función sobre ningún número distinto de los de sus propios clientes, reservándose la consultante el derecho a inspeccionar el efectivo cumplimiento de esta cautela y a resolver el contrato en caso contrario.

Al propio tiempo, no debe ignorarse que la sentencia de la Audiencia Nacional de 17 de septiembre de 2008 ha señalado que la mera referencia a un número de teléfono “ayuno de otras circunstancias que identifiquen o pudiesen permitir identificar al titular del mismo impide que pueda encajarse en la definición legal de dato de carácter personal”.

En el supuesto analizado, el sistema se implantaría, conforme a la propia naturaleza de la consultante, en relación con números de telefonía móvil, respecto de los que no existen en este momento directorios que permitan mediante su simple consulta la identificación del abonado a partir de su número telefónico, de suerte que únicamente en caso de que se trate de clientes de las entidades financieras receptoras del resultado de la aplicación de la función HASH sobre el número telefónico será posible concluir, a la luz de la sentencia citada, que nos encontramos terminantemente ante dato de carácter personal. En todo caso, como se ha señalado reiteradamente, la consulta prevé expresamente que la entidad financiera sólo podría aplicar la función HASH a los datos correspondientes a los números telefónicos de sus propios clientes, quedándole vedada la posibilidad de aplicar la función a números distintos de aquéllos y encontrándose sujeta a la posibilidad de que la consultante controle el cumplimiento de esta obligación y, en su caso, pueda proceder a la resolución unilateral del contrato.

En consecuencia, las transmisiones de información que se realizarán entre las entidades financieras y la consultante no se encontrarían sometidas a lo dispuesto en la Ley Orgánica 15/1999, dado que, por una parte, los datos referidos a los centros servidores de SMS no se corresponden con personas físicas y, por otra, el dato resultante de la aplicación de la función HASH sobre un determinado número de teléfono no permite la identificación del mismo por parte de la entidad financiera destinataria de la información, puesto que ese dato identifica a una pluralidad de números de teléfono que pueden corresponderse o no con los de clientes de la entidad y pueden igualmente referirse no sólo al número de un cliente determinado sino a varios de ellos.

IV

Deben ahora analizarse los restantes tratamientos de datos que tendrán lugar en el supuesto descrito en la consulta, esto es, el realizado por la entidad consultante, que vinculará los datos referidos a los centros servidores con la cabecera del mensaje, extrayendo la información referida a los destinatarios de los mensajes SMS en caso de no coincidir la información con la facilitada por la entidad financiera, y el efectuado por ésta última a partir de la información recibida de la consultante y relacionado, según se ha venido indicando, con los datos de los clientes que hubieran recibido los mensajes en los que no se produjera la citada coincidencia.

En cuanto al tratamiento efectuado por la entidad financiera, una vez detectados el o los números telefónicos de los clientes que pudieran haberse visto implicados en el supuesto presuntamente fraudulento, el artículo 6.1 de la Ley Orgánica 15/1999 dispone que “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”, si bien añade el artículo 6.2 que “No será preciso el consentimiento cuando los datos de carácter personal (...) se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”.

En el presente caso, de la información facilitada en la consulta parece deducirse que el tratamiento que llevarían a cabo las entidades podría implicar el análisis del carácter fraudulento de la información remitida a sus clientes o incluso la advertencia a los mismos de que tal circunstancia se ha produciendo, a fin de evitar la causación a los mismos de algún perjuicio como consecuencia de la conducta fraudulenta derivada de la presunta suplantación de la identidad de la entidad financiera en la remisión del mensaje SMS.

De este modo, el mencionado tratamiento podría incardinarse en los que la entidad llevase a cabo en el marco de la relación contractual mantenida con sus clientes, a fin de garantizar un adecuado cumplimiento, desarrollo y control de la misma, por lo que cabría entenderlo amparado por el artículo 6.2 de la Ley Orgánica 15/1999.

En todo caso, esta circunstancia no exonera a la entidad financiera de informar a los clientes acerca del mencionado tratamiento, en cumplimiento de lo establecido en el artículo 5.1 de la Ley Orgánica 15/1999. En este sentido, la consulta prevé que las entidades deberán informar a sus clientes acerca del tratamiento de sus datos “con la finalidad de evitar la suplantación de personalidad en las comunicaciones móviles que la entidad bancaria les realice y únicamente con dicha finalidad”, aclarando que dicho tratamiento no se referirá a los contenidos de los mensajes, por lo que se daría cumplimiento a lo exigido por dicho precepto.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

V

Resta por último hacer referencia al tratamiento de datos que la consultante llevará a cabo con la finalidad de detectar la existencia de una suplantación y aplicar sobre los números de teléfono de los destinatarios de dicha suplantación la función HASH a la que se ha hecho referencia.

Para llevar a cabo dicho tratamiento, y una vez detectada la existencia de una irregularidad en la relación centro servidor/cabecera del mensaje, la consultante deberá proceder al tratamiento de los datos identificativos del número del destinatario, a fin de proceder con posterioridad a la aplicación de la función y a la remisión de los datos a la entidad financiera.

Debe tenerse en cuenta que en el presente caso el tratamiento se referirá además a datos de tráfico, toda vez que el artículo 64 a) del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, define como tales “cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación”, siendo así que en tal concepto se incluirán los números telefónicos del remitente y destinatario del SMS así como, en su caso, la mera cabecera del mensaje.

Pues bien, el artículo 65 del mencionado Reglamento regula los posibles usos que podrán darse a los datos de tráfico por parte de los prestadores de servicios de comunicaciones electrónicas, estableciendo en su apartado 1 que “los operadores deberán eliminar o hacer anónimos los datos de carácter personal sobre el tráfico referidos a una comunicación y relacionados con los usuarios y los abonados que hayan sido tratados y almacenados para establecer una comunicación, en cuanto ya no sean necesarios a los efectos de su transmisión, sin perjuicio de lo dispuesto en los apartados siguientes”.

El artículo 65.2 añade que “los datos de tráfico que fueran necesarios para realizar la facturación y los pagos de las interconexiones podrán ser tratados únicamente durante el plazo en que pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable. Transcurrido dicho plazo, los operadores deberán eliminar o hacer anónimos los datos de carácter personal, en los términos del apartado 1”.

Por último, el artículo 65.5 limita el acceso a estos datos, al prever que “el tratamiento de los datos de tráfico, de conformidad con los apartados

anteriores, sólo podrá realizarse por las personas que actúen bajo la autoridad del operador prestador del servicio o explotador de la red que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas, de la prestación de un servicio con valor añadido o de suministrar la información requerida por los jueces y tribunales, por el Ministerio Fiscal o por los órganos o entidades que pudieran reclamarla en virtud de las competencias atribuidas por la Ley 32/2003, de 3 de noviembre" y concluye que "en todo caso, dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades".

De lo señalado en el último inciso que acaba de reproducirse se desprende que los operadores sí podrían tratar datos de tráfico en lo que resulte necesario para la detección del fraude, toda vez que el artículo 65.5 se refiere a tal finalidad y habilita en su último inciso el tratamiento, si bien limitado a tal finalidad.

De este modo, es posible considerar que el tratamiento de los datos de tráfico asociados a una determinada comunicación electrónica que pudiera considerarse fraudulenta, tanto en lo que afecta a las normas reguladoras de las comunicaciones electrónicas como a las aplicables a las relaciones subyacentes a la propia comunicación puede entenderse amparada en el necesario control del adecuado cumplimiento por parte del operador de las exigencias contenidas en la legislación reguladora de este tipo de comunicaciones, pudiendo en consecuencia entenderse igualmente amparada en el artículo 6.2 de la Ley Orgánica 15/1999 y en las previsiones contenidas en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y, en consecuencia, amparada asimismo por el artículo 6.1.

Debe en este sentido tenerse en cuenta que el tratamiento de datos de los destinatarios de las comunicaciones presuntamente fraudulentas únicamente sería llevado a cabo, en los términos descritos en la consulta, por la propia consultante, dado que la misma no facilitaría a las entidades financieras más que el resultado de aplicar al número telefónico la función HASH a la que se ha venido haciendo referencia, siendo así que el resultado facilitado no identifica unívocamente, como se ha indicado, a la línea destinataria del mensaje presuntamente fraudulento, sino a una pluralidad de líneas.

VI

A la vista de todo lo que se ha venido indicando en el presente informe, cabe concluir que la actividad descrita en la consulta no resulta contraria a lo dispuesto en la Ley Orgánica 15/1999, siempre que se cumplan las condiciones que en ella se describen y, en particular, las mencionadas en su apartado IV

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

bajo la rúbrica “medidas de seguridad a implementar”.