IDENTIFICACIÓN DE TERMINALES O DISPOSITIVOS DE CONECTIVIDAD AL AMPARO DEL ART. 588 TER M DE LA LEY ORGÁNICA 13/2015

JULIO 2016

IDENTIFICACIÓN DE TERMINALES O DISPOSITIVOS DE CONECTIVIDAD AL AMPARO DEL ART. 588 TER M DE LA LEY ORGÁNICA 13/2015

1.- EL IMSI Y EL IMEI EN ESTÁNDAR EUROPEO DE TELECOMUNICACIONES... 2

1.1.- DEFINICIÓN DE IMSI E IMEI 2

1.2.- EL USO DEL IMSI Y DEL IMEI EN LA RED CELULAR DE COMUNICACIONES MÓVILES POR PARTE DE LAS OPERADORAS 3

2.- IMSI E IMEI COMO DATOS IDENTIFICATIVOS DE ABONADOS Y TERMINALES O DISPOSITIVOS DE CONECTIVIDAD 4

3.- CONSERVACIÓN DEL IMSI Y EL IMEI EN LOS REGISTROS DE DATOS DE LAS OPERADORAS 5

4.- ACCESO Y CESIÓN DE LOS DATOS DE IMSI E IMEI GENERADOS, TRATADOS O CONSERVADOS POR LAS OPERADORAS 6

4.2.- CESIÓN POR PARTE DE LAS OPERADORAS DE CÓDIGOS IMSI E IMEI CONSERVADOS EN VIRTUD DE LA LEY 25/2007 7

4.1.- CESIÓN POR PARTE DE LAS OPERADORAS DE CODIGOS IMSI E IMEI OBRANTES EN REGISTROS NO VINCULADOS A PROCESOS DE COMUNICACIÓN 8

4.3.- GENERACIÓN EN LÍNEA Y CESIÓN POR PARTE DE LAS OPERADORAS DEL IMSI E IMEI DE UN TERMINAL O DISPOSITIVO DE CONECTIVIDAD 8

IDENTIFICACIÓN DE TERMINALES O DISPOSITIVOS DE CONECTIVIDAD AL AMPARO DEL ART. 588 TER M DE LA LEY ORGÁNICA 13/2015

1.- EL IMSI Y EL IMEI EN ESTÁNDAR EUROPEO DE TELECOMUNICACIONES

1.1.- DEFINICIÓN DE IMSI E IMEI

Según los estándares europeos relativos a sistemas de telecomunicaciones celulares digitales, establecidos por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) [1], un dispositivo de comunicaciones móviles celulares plenamente operativo, denominado en el lenguaje coloquial “Teléfono Móvil” y en el técnico “Estación Móvil” (Mobile Station, MS), se compone materialmente de dos elementos esenciales. En primer lugar, el terminal o equipo electrónico móvil (Mobile Equipment, ME) dotado de pantalla, procesador, memoria, módem de comunicaciones y batería. En segundo lugar, el módulo de identificación de usuario, más conocido como “tarjeta SIM” (Subscriber Identity Module) [2]. Esta tarjeta SIM es intercambiable entre los diferentes terminales móviles existentes en el mercado y contiene en su chip digital la información necesaria para identificar y autenticar al abonado, incluido el International Mobile Subscriber Identity (IMSI) [3], el cuál identifica de forma inequívoca al abonado en la red celular [4]. Sin un IMSI válido los servicios de telefonía móvil no serán accesibles, salvo en el caso de llamadas de emergencia [2]. De hecho, el IMSI está principalmente previsto para obtener información del uso de la red por el abonado a los efectos de facturación individual [5].

En lo que se refiere a la identificación del terminal o equipo electrónico de comunicaciones (ME), los estándares europeos establecen el código conocido como International Mobile Estation Equipment Identity (IMEI) como el número único asignado individualmente a cada equipo o terminal en la red, que debe ser incondicionalmente implementado en el terminal por su fabricante y que ha de ser inalterable después de su producción. Este código es necesario para obtener información acerca de la presencia de específicos terminales o equipos en la red, independientemente de los abonados que estén haciendo uso de ellos [5].

Mientras que un terminal móvil puede ser suministrado a un usuario en cualquier comercio del sector electrónico o por su proveedor de servicios de telecomunicaciones, una tarjeta SIM operativa siempre habrá de ser suministrada al abonado por su compañía proveedora de servicios de telecomunicaciones, conteniendo la ya citada información que le identificará en la red, IMSI incluido, y que le dará acceso a los servicios contratados. Por este motivo, un proveedor de servicios de telecomunicaciones contará en sus bases de datos de clientes y de facturación con los datos personales del abonado, de la SIM y el IMSI suministrado y, **en caso de haber suministrado también un terminal móvil**, el IMEI del mismo.

1.2.- EL USO DEL IMSI Y DEL IMEI EN LA RED CELULAR DE COMUNICACIONES MÓVILES POR PARTE DE LAS OPERADORAS

El IMSI es, por tanto, el código de identificación por excelencia en la red de comunicaciones móviles celulares, que da acceso al abonado a los servicios contratados y que permite la facturación correspondiente por parte del proveedor. Por ello, es generalizado su uso en los procesos de identificación, autenticación y cifrado que se ejecutan en la red con ocasión de las múltiples causas de establecimiento de conexión existentes entre la estación móvil y la misma, tanto vinculadas a procesos de comunicaciones del abonado, como desvinculadas de los mismos [6].

Por otra parte, en lo que se refiere al IMEI, la especificación técnica del estándar correspondiente [5] establece que cada operador puede hacer un uso administrativo del mismo, en concreto, estableciendo registros de IMEIs agrupados en listas blancas, grises o negras, de las cuales podrá hacer un uso discrecional. Las listas blancas contienen la identificación de terminales autorizados para el uso de la red y los servicios de telecomunicaciones. Las negras contienen las identificaciones de terminales con uso de la red prohibido. Y, por último, las grises, contienen los datos de terminales que son monitorizados por la red para evaluación u otros propósitos. La prohibición de uso o la monitorización de un terminal, puede responder al objeto de prevenir el robo y comercio ilícito de terminales o al de detectar modelos de terminales que no serán compatibles con la red por motivos técnicos. De hecho, la GSM Asociation creó en 2005 el International Mobile Equipment Identity Database (IMEI DB) para el intercambio de listas de IMEIs entre operadores y fabricantes [7]. Estos servicios permiten a los operadores, por ejemplo, chequear si los IMEIs de los terminales móviles empleados por los abonados en su red han sido incluidos en la lista negra, como sustraídos, por otro operador de cualquier lugar del planeta, pudiendo así incluirlos en su propia lista negra y denegarles sus servicios.

En relación con todo lo anterior, la instrucción técnica del estándar correspondiente [5] establece que deberá ser posible que la red lleve a cabo un procedimiento de chequeo del IMEI del terminal en cada intento de acceso a la red que este haga [8], excepto en aquellos que se produzcan para cerrar la conexión [9]. Del mismo modo deberá ser posible realizar el chequeo de IMEI en cualquier momento durante una llamada establecida cuando esté disponible un recurso radio dedicado, de acuerdo con la política de seguridad del operador de la red. También deberá ser posible realizar el chequeo de IMEI cuando esté registrado en una sesión de datos de Internet (Internet Media Service, IMS). De hecho, si el resultado del chequeo del IMEI contra la lista negra del operador determina que se trata de un terminal con uso de red prohibido, el resultado será el mismo que cuando se produce un error en la autenticación de un abonado mediante su tarjeta SIM y su IMSI, por lo que se le denegará el establecimiento de llamadas o sesiones de Internet, así como la ejecución de otras actividades de red. Es preciso señalar que el tiempo verbal empleado por la instrucción técnica es “deberá ser posible”, por lo que no se establece obligatoriedad en la ejecución de los chequeos de IMEI con estos fines, de hecho, se aclara que se harán “de acuerdo con la política de seguridad del operador”.

Por otra parte, se establece que el IMEI y el IMEISV [10] son elementos de información de identificación móvil que deberán ser comunicados por la estación móvil a la red, al menos en los siguientes casos:

- Cuando el usuario realice una llamada de emergencia desprovisto de una SIM o con una SIM o un IMSI no válido.
- Cuando se ejecute un procedimiento de configuración del modo de cifrado.
- Cuando se ejecute un procedimiento de autenticación y cifrado en el ámbito de conexiones GPRS [11].

Los dos últimos casos son procesos que la red ejecuta automáticamente, y que suelen establecerse prácticamente cada vez que se produce un establecimiento de conexión entre la estación móvil y la red, que lleva consigo procedimientos de autenticación y cifrado para garantizar la confidencialidad de datos así catalogados [12]. Es preciso incidir en que estos establecimientos de conexión no se limitan a momentos en los que el usuario o abonado inicia el proceso para realizar una comunicación propiamente dicha, sino que pueden tener lugar por causas desvinculadas las comunicaciones del abonado y que son relativas a procesos de red necesarios para el mero mantenimiento de la operatividad de la estación móvil [6].

2.- IMSI E IMEI COMO DATOS IDENTIFICATIVOS DE ABONADOS Y TERMINALES O DISPOSITIVOS DE CONECTIVIDAD

A la vista del apartado anterior, queda claro que, desde el punto de vista del estándar ETSI de telecomunicaciones celulares, tanto el IMSI como el IMEI, son códigos identificativos de abonados y terminales o dispositivos de conectividad, respectivamente.

En el ámbito normativo jurídico, tanto a nivel europeo como nacional, veremos a continuación que la perspectiva es considerablemente análoga.

En el ámbito europeo, la derogada *Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que modifica la Directiva 2002/58/E* [13], establecía en su art. 5.1.e.2 como datos necesarios para la identificación del equipo de comunicación empleado en el ámbito de la telefonía móvil el IMSI y el IMEI, entre otros [14].

Esta catalogación fue traspuesta, prácticamente de manera literal, a la *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, concretamente en su art. 3.1.e.2º, y que goza de pleno vigor en el Ordenamiento Jurídico Español.

Por su parte, también en el ámbito nacional, la *Ley 9/2014, de 9 de mayo, de Telecomunicaciones*, establece en su art. 39.5.a, relativo al deber de los sujetos obligados de facilitar a los agentes facultados los datos de la identidad o identidades del sujeto objeto de la medida de interceptación, que *"Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso."*

La propia *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, identifica en su art. 588 ter l el IMSI y el IMEI como *"códigos de identificación o etiquetas técnicas del aparato de telecomunicaciones o de alguno de sus componentes".*

Puede concluirse, por tanto, que para la plena identificación de un "Teléfono Móvil" como terminal o dispositivo de conectividad completo, que se compone por una tarjeta SIM y un terminal móvil, en el sentido recogido en el art. 588 ter m. de la L.O. 13/2015, es necesario conocer tanto el IMSI alojado en la primera, como el IMEI del segundo.

3.- CONSERVACIÓN DEL IMSI Y EL IMEI EN LOS REGISTROS DE DATOS DE LAS OPERADORAS

Del análisis realizado en los apartados anteriores puede concluirse que, tanto el IMSI como el IMEI, son códigos generados por la red de telecomunicaciones celulares móviles que las operadoras gestionan y administran para el correcto funcionamiento de la misma y para otros fines de su interés. Los procesos en los que se emplean tales códigos identificativos pueden estar vinculados a las comunicaciones de los abonados propiamente dichas, como es el caso del establecimiento de una llamada de voz o de una sesión de Internet. Pero también se dan procesos desvinculados de las mismas, como son los procesos necesarios para el simple mantenimiento de la operatividad de la red y las estaciones móviles, o los procesos necesarios para la facturación o para garantizar la seguridad de los abonados.

La cuestión planteada en este epígrafe es determinar cuándo, y en qué condiciones, las operadoras están obligadas a conservar o no dichos datos de identificación de terminales y abonados y si, aun no estando obligadas, los conservan igualmente por otros intereses.

La Ley 25/2007, establece en su art. 3 los datos que deben ser conservados por los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones en el marco de su prestación de servicios. En la redacción del art. 3 se vinculan todos los datos de obligada conservación a un proceso de comunicación con un origen y un destino de la misma. Concretamente, en el art. 3.d de la Ley 25/2007, que establece la obligatoriedad de conservación de los datos necesarios para identificar el tipo de comunicación, se enumeran los mismos. Con respecto a la telefonía móvil se especifican los siguientes tipos de comunicaciones: *"el servicio telefónico utilizado: tipo de* ***llamada*** *(trasmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o* ***servicios de mensajería o multimedia*** *empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia)"*. En ningún caso, se hace referencia en la Ley 25/2007 a tipos de comunicaciones entre una estación móvil y la red distintos a los relacionados, que no tengan por objeto el establecimiento de una comunicación con otro usuario o abonado [6]. Por ejemplo, no existe obligación de conservar datos relativos a las conexiones realizadas por una estación móvil al ser encendida y registrarse en la red o al realizar, con ocasión de desplazarse, un cambio en la antena que le da servicio. Algo que confirma esta interpretación es que la propia norma se ve obligada a especificar en el art. 3.1.e).1.vi) que será un dato de obligada conservación: *"En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación y la etiqueta técnica de localización (el identificador de celda) desde la que se haya activado el servicio".* Este es el único caso de proceso de red desvinculado de un acto de comunicación, que ha sido expresamente recogido en el texto de la misma.

Independientemente de la obligación legal de conservar los datos especificados en el párrafo anterior, es lógico pensar que las operadoras conservan y tratan, por sus propios intereses y los de sus abonados, datos identificativos de abonados y terminales (IMSI e IMEI). Así pues, el IMSI es conservado, por ejemplo, tanto en los registros de uso de la red con fines de facturación, como en las fichas de clientes, como en la propia red para realizar la autenticación de usuarios contra los registros de abonados autorizados [15]. El IMEI, por su parte, puede quedar almacenado en los registros de facturación de ventas de terminales o en las fichas de cliente cuando se trata de terminales suministrados por el propio operador al abonado, o registrado en listas blancas, negras y grises de IMEIs, que los propios operadores pueden intercambiar entre sí, para la realización de chequeos en línea de los IMEI de terminales móviles registrados en sus redes en un momento dado. Esto último con el objeto de detectar y bloquear, en su caso, el uso de terminales robados o, también, de detectar y evaluar el uso en su red de determinados modelos de terminales. Por otra parte, no se debe olvidar el

gran número de conexiones generadas entre las estaciones móviles y la red, no vinculadas a comunicación alguna [6], excluidas por tanto de los tipos de comunicación objeto de conservación según el art. 3.d de la Ley 25/2007 relacionados en el párrafo anterior, y que llevan consigo un proceso de identificación del IMSI y/o del IMEI. Muy probablemente, las operadoras conserven registros de estas conexiones por un tiempo determinado, por motivos de estudios para la optimización del rendimiento de la red o de otro tipo.

4.- ACCESO Y CESIÓN DE LOS DATOS DE IMSI E IMEI GENERADOS, TRATADOS O CONSERVADOS POR LAS OPERADORAS

El art. 588 ter m de la Ley Orgánica 13/2015, que versa sobre la identificación de titulares o terminales o dispositivos de conectividad, establece que el **Ministerio Fiscal o la Policía Judicial**, cuando en el ejercicio de sus funciones lo necesiten, **podrán dirigirse** directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, **sin** necesidad de previa **autorización judicial**, **para recabar los datos de titularidad** de un número de teléfono o de cualquier otro medio de comunicación o, en sentido inverso, el número de teléfono o los **datos identificativos de cualquier medio de comunicación**.

Por su parte, el art. 588 ter j, de esa misma Ley Orgánica, que se refiere a datos obrantes en archivos automatizados de los prestadores de servicios, establece en su apartado 1 que *"Los **datos electrónicos conservados** por los prestadores de servicios o personas que faciliten la comunicación **en cumplimiento de la legislación** sobre retención de dato relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren **vinculados a procesos de comunicación**, solo podrán ser cedidos para su incorporación al proceso con **autorización judicial**".*

Siendo el IMSI y el IMEI, como ha quedado ya acreditado, datos necesarios para la identificación de una estación móvil ("Teléfono Móvil") como medio de comunicación, surge en este punto la duda de si existe algún tipo de contradicción entre el art. 588 ter j (y por remisión la Ley 25/2007) por un lado y el art. 588 ter m por otro, en relación con la necesidad o no de previa autorización judicial para el acceso por parte del Ministerio Fiscal o la Policía Judicial a dichos datos, obrantes en los archivos de los prestadores de servicios o disponibles en línea en sus redes.

Procede traer nuevamente a colación el contenido del art. 588 ter l de la Ley Orgánica 13/2015, que trata sobre la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes. En su apartado primero se faculta a los agentes de Policía Judicial para, sin el requisito de previa autorización judicial, valerse de artificios técnicos que permitan acceder al conocimiento del IMSI e IMEI de la estación móvil empleada por un abonado. Este tipo de procedimiento técnico tiene lugar realizando la monitorización del espectro radioeléctrico que permiten acceder a los códigos identificativos mencionados de forma desvinculada de cualquier tipo de comunicación establecida por el abonado, que pueda estar amparada por el derecho al secreto de las comunicaciones o por la normativa de conservación de datos de ley 25/2007.

Por tanto, es razonable interpretar que la obtención de los códigos IMSI e IMEI, como datos identificativos de la tarjeta SIM del abonado (dispositivo de conectividad) y del el terminal móvil empleado, por parte de la Policía Judicial, cuando no estén vinculados a los procesos de comunicación, no supone en sí misma una injerencia en el derecho al secreto de las comunicaciones, ni una injerencia en el derecho a la intimidad de suficiente envergadura, como para que sea exigido el requisito de previa autorización judicial para el acceso a los mismos por parte del Ministerio Fiscal o de la Policía Judicial, y todo ello en virtud del art. 588 ter m de la Ley Orgánica 13/2015.

4.2.- CESIÓN POR PARTE DE LAS OPERADORAS DE CÓDIGOS IMSI E IMEI CONSERVADOS EN VIRTUD DE LA LEY 25/2007

Las operadoras tienen la obligación de conservar los datos generados o tratados en el marco de su prestación de servicio en virtud de la *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*. Concretamente, la redacción literal de su art. 3.1.e.2º relativo a los datos objeto de conservación obligada y, específicamente en lo que atañe al IMSI y al IMEI, es la siguiente:

"1. Los datos que deberán conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:
……
e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser equipo de comunicación:
……
2º Con respecto a la telefonía móvil:
……
ii) La identidad internacional del abonado móvil (IMSI) ***de la parte que efectúa la llamada****.*
iii) La identidad internacional del equipo móvil (IMEI) ***de la parte que efectúa la llamada****.*
iv) La IMSI ***de la parte que recibe la llamada****.*
v) La IMEI ***de la parte que recibe la llamada****.*
……"

De esta redacción y de la del resto del art. 3, se deduce que el origen y fundamento de la obligación de conservar dichos datos es su vinculación a un proceso de comunicación de un tipo determinado, concretada en el tiempo, con un origen y un destino, una duración e, incluso, asociada a una localización espacial. De hecho, es el establecimiento de una comunicación, el evento en la red que desencadena el registro y almacenamiento de estos datos asociados en los registros de datos conservados de la operadora.

En concreto, el art. 3.1.d.1º establece que los datos necesarios para identificar el tipo de comunicación en el caso de la telefonía móvil, son los siguientes:

- Llamadas (transmisión de voz, buzón vocal, conferencia, datos).
- Servicios suplementarios (incluido el reenvío o transferencia de llamadas).
- Servicios de mensajería o multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

Por tanto, puede entenderse que son estos tipos de procesos de comunicación, y sólo estos, los que están afectados por las garantías establecidas por la norma.

La cesión por parte de las operadoras de los datos de IMSI e IMEI conservados por estar vinculados a comunicaciones de los tipos descritos, cuando se haga en unión, no sólo de esta información de tipo de comunicación, sino también del resto de datos asociados como origen y destino de la comunicación, fecha y hora, duración y localización, debe entenderse, sin duda, sujeta a lo establecido en el art. 6 de la Ley 25/2007, que establece en su apartado 1 el requisito de la previa autorización judicial. Criterio éste reiterado por la Ley Orgánica 13/2015 en su art. 588 ter j mediante remisión literal a la legislación sobre retención de datos relativos a las comunicaciones electrónicas. El apartado 2 del mismo art. 6, establece que la cesión de la mencionada información sólo podrá efectuarse a los agentes de las Fuerzas y Cuerpos de Seguridad, a los funcionarios de la División Adjunta de Vigilancia Aduanera y al personal del Centro Nacional de Inteligencia, todo ello cuando desempeñen determinadas de sus competencias.

Pero, es preciso profundizar en lo establecido en el art. 6 de la Ley 25/2007 para dimensionar el alcance dicha limitación en la cesión de los datos conservados, en el sentido de que en él no se restringe el acceso por parte de la propia operadora a los datos conservados

que ella misma registra en cumplimiento de lo establecido en la norma, sino que lo que se limita es la cesión por su parte de los datos a los agentes facultados.

Así pues, la injerencia en el derecho al secreto de las comunicaciones, y también, la sujeción a las garantías establecidas por la ley 25/2007 y, en concreto, a la de previa autorización judicial en lo que se refiere a la cesión de estos datos a los agentes facultados por parte de las operadoras, parece carecer de fundamento si están totalmente desvinculados de la comunicación que los originó, consistiendo exclusivamente en la aportación de datos de IMSIs o IMEIs disociados de proceso de comunicación material alguno concretado en el tipo, tiempo o espacio e igualmente disociados de otros datos de destino u origen de dicho proceso de comunicación.

Podría considerarse, por tanto, que el conocimiento de un dato de IMSI o IMEI por parte del Ministerio Fiscal o la Policía Judicial, en las condiciones fijadas en el art. 588 ter m, no supondría injerencia alguna en el secreto de las comunicaciones o esté afectado por el art. 6 de la Ley 25/2007, siempre y cuando sea presentado por la operadora a los agentes facultados disociado de proceso de comunicación alguno al que vincular dicho dato, y pese a que la operadora haya precisado acceder a sus propios registros de datos conservados para extraer dicha información y cederla ya disociada.

4.1.- CESIÓN POR PARTE DE LAS OPERADORAS DE CODIGOS IMSI E IMEI OBRANTES EN REGISTROS NO VINCULADOS A PROCESOS DE COMUNICACIÓN

Se ha comprobado cómo, con independencia de los registros de almacenamiento de datos conservados en virtud de la Ley 25/2007, las operadoras pueden contar con otro tipo de registros en los que se conservan datos de IMSI e IMEI no vinculados a procesos de comunicación.

La legalidad de la cesión de dichos datos de identificación por parte de la operadora sin previa autorización judicial al Ministerio Fiscal o a la Policía Judicial, en virtud y en las condiciones establecidas en el art. 588 ter m de la Ley Orgánica 13/2015 es, en este caso, ciertamente no cuestionable, ya que ni tienen su origen en procesos de comunicación, ni son conservados como parte integrante de los registros de datos de obligada conservación conforme a la Ley 25/2007.

4.3.- GENERACIÓN EN LÍNEA Y CESIÓN POR PARTE DE LAS OPERADORAS DEL IMSI E IMEI DE UN TERMINAL O DISPOSITIVO DE CONECTIVIDAD

Con independencia de los datos de IMSI e IMEI registrados y almacenados por las operadoras, sean vinculados a procesos de comunicación y conservados en virtud de la normativa de conservación de datos relativos a comunicaciones electrónicas, o sean desvinculados de procesos de comunicación y conservados por su propia iniciativa por motivos comerciales o de otra índole, se ha constatado que toda red de comunicaciones digitales celulares es capaz de recabar en un momento dado, de forma totalmente desvinculada de proceso de comunicación alguno del abonado, el IMSI y el IMEI de una estación móvil operativa a la que esté prestando servicio.

Por tanto, sería factible que la operadora, **mediante un proceso de red en línea desvinculado de comunicación alguna del abonado**, identifique el IMSI y el IMEI de una estación móvil que se encuentre operativa en su red, todo ello, en cumplimiento de una petición del Ministerio Fiscal o la Policía Judicial efectuada al amparo del art. 588 ter m y sin necesidad de previa autorización judicial.

[1] El Instituto Europeo de Estándares de Telecomunicaciones (ETSI) produce estándares de aplicación global para las tecnologías de información y telecomunicaciones, incluidas tecnologías fijas, móviles, radio, convergentes, de difusión ancha e Internet. Está oficialmente reconocido por la Unión Europea como Organización de Estándares Europeos. Se trata de una organización sin ánimo de lucro que cuenta con más 800 organizaciones como miembros en todo el mundo, distribuidas en 66 países y 5 continentes.

[2] ETS 300 509 (GSM 02.17). 1994. European digital celular telecommunications system (Phase 2); Subscriber Identity Modules (SIM) Functional characteristics. Sophia Antipolis CEDEX: European Telecommunications Standards Institute, Septiembre 1994. 10 p.

[3] GSM 03.03 (TS/SMG-030303Q). 1996. Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification. Sophia Antipolis CEDEX: European Telecommunications Standards Institute, Marzo 1996. 9 y 17 p.

[4] Según el estándar ETS 300 509 (GSM 02.17), se trata de códigos digitales almacenados en la memoria digital del chip, no identificables a simple vista, entre los que, además del IMSI, se encuentran otros datos como las claves de autenticación del abonado, datos temporales de red, datos relativos al servicio contratado como preferencias de lenguaje o avisos de carga, o el código PIN, que provee protección contra el uso no autorizado de la estación móvil.

[5] ETSI TS 122 016 v13.0.0. 2016. Digital cellular telecommunications systems (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; International Mobile station Equipment Identities (IMEI) (3GPP TS 22.016 version 13.0.0 Release 13). Sophia Antipolis CEDEX: European Telecommunications Standards Institute, Febrero 2016. 5 y 6 p.

[6] Según la especificación técnica ETSI TS 142 009 (689 p), estas causas de conexión, no vinculadas a una comunicación del usuario propiamente dicha, pueden ser, por ejemplo, el registro en la red que se produce al encender la estación móvil, su desconexión de la red, un registro periódico, la ejecución de un proceso de red de actualización de localización, etc.

[7] La GSM Asociation (GSMA), creada en 1995, y que representa los intereses de los operadores nóveles a nivel mundial, estando integrada por cerca de 800 operadores y más de 250 compañías del sector, incluyendo fabricantes y proveedores de terminales móviles y software, mantiene desde 2005 un sistema único conocido como International Mobile Equipment Identity Database (IMEI DB), que es un base de datos global central que contiene información básica relativa a los rangos de números de serie (IMEI) de millones de dispositivos móviles (incluidos terminales móviles, módems de comunicaciones de ordenadores portátiles, etc) que son utilizados en la red móvil mundial. Uno de los principales objetivos de esta herramienta es Los operadores pueden compartir sus listas (negras, blancas o grises) que quedan almacenadas en el Central Equipment Identity Register (CEIR), de forma que los terminales incluidos en su lista negra tampoco podrán acceder a las redes del resto de operadores. La GSMA ofrece acceso gratuito a operadores y autoridades a estas prestaciones de listas negras que considera de gran eficacia para la labor de agentes de la seguridad pública y para la tranquilidad de los abonados. Los operadores podrán utilizar las prestaciones de la lista negra para monitorizar un terminal incluido en su lista gris.

[8] La especificación técnica 3GPP TS 22.016 (ETSI TS 122 016 v13.0.0) no hace distinción entre tipos de intentos de acceso a la red realizados con ocasión de un establecimiento de llamada o sesión de datos o con ocasión de procesos no vinculados a una comunicación concreta como puedan ser procesos de actualización de localización de la estación móvil, registro en la red u otros necesarios para la operatividad de dispositivo de conectividad.

[9] La especificación técnica 3GPP TS 22.016 (ETSI TS 122 016 v13.0.0) establece que no será obligatorio que la red pueda chequear el IMEI de un terminal móvil en los intentos de acceso a la red que consistan en un “IMSI detach”. El “IMSI detach” es el proceso establecido para realizar la desconexión de la red cuando una estación móvil es desactivada, cuando la tarjeta SIM es retirada del terminal móvil o como parte de un procedimiento de inactividad eCall

(vid. ETSI TS 124 008 v13.5.0. 2016. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008 version 13.5.0 Release 13). Sophia Antipolis CEDEX: European Telecommunications Standards Institute, Abril 2016. Pag. 99.).

[10] El IMEISV está compuesto por el IMEI y por la versión de software que emplea el terminal (Software Version, SV), según la especificación técnica GSM 03.03 (TS/SMG-030303Q).

[11] ETSI TS 124 008 v13.5.0. 2016. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008 version 13.5.0 Release 13). Sophia Antipolis CEDEX: European Telecommunications Standards Institute, Abril 2016. Pag. 448 y 449.

[12] ETSI TS 142 009. 2006 v4.1.0. 2006. Digital celular telecommunications system (Phase 2+); Security aspects (3GPP TS 42.009 version 4.1.0 Release 4). Sophia Antipolis CEDEX: European Telecommunications Standards Institute, Junio 2006. En esta especificación técnica se establece que la identidad de abonado (IMSI), los datos de las comunicaciones del usuario así como la información de señalización relativa a la estación móvil y que es empleada por la red para mantener su operatividad, son confidenciales.

[13] La Directiva 2006/24/CE fue derogada por la Sentencia del Tribunal de Justicia (Gran Sala) de la Unión Europea, de 8 de abril de 2014, Digital Rights Ireland (C-293/12) contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landersregierung (C-594/12) y otros. No obstante, la normativa nacional, consecuencia de su trasposición en su día al Ordenamiento Jurídico Español, permanece en vigor en la actualidad.

[14] Vid. Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE. Art. 5.1.e.2.

[15] Es el caso de los registros Home Location Register (HLR) y Visitor Locaton Register (VLR) (vid. Recomendation GSM 03.02. European digital celular telecommunication system (Phase 1); Network Architecture. Valbonne Cedex (France): European Telecommunictions Standards Institute, Febrero 1992. Pag. 2 y 3), empleados respectivamente por la red para registrar y grabar los datos de usuarios, como por ejemplo los desidentificación, y para facilitar, por ejemplo, información necesaria para el establecimiento de llamadas desde una estación móvil en roamig.