FISCALÍA GENERAL DEL ESTADO
Unidad de Criminalidad Informática

Dictamen nº 1/19 de la Unidad de Criminalidad Informática de la Fiscalía General del Estado acerca del alcance de la reclamación de datos de identificación de titulares, terminales y/o dispositivos de conectividad prevista en el nuevo artículo 588 ter m de la Ley de Enjuiciamiento Criminal

Tras la entrada en vigor de la reforma procesal operada por la LO 13/2015 de 5 de octubre, esta Unidad Central del Área de Especialización en Criminalidad Informática ha tenido conocimiento de que se están generando discrepancias acerca de los datos que, al amparo del nuevo artículo 588 ter m), pueden entregar los prestadores de servicios de telecomunicaciones, de acceso a la red o de servicios de la sociedad de la información a petición directa de la Policía Judicial o del Ministerio Fiscal –es decir, sin autorización judicial- con fines de investigación.

Recordemos que la mencionada Ley Orgánica incorporó el artículo 588 ter m en la Ley de Enjuiciamiento Criminal con el siguiente contenido : *Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, 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, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.*

Nótese que en el citado precepto se hace referencia no solo a la obtención de la identidad de quien sea el titular de un número de teléfono o de cualquier otro medio de comunicación, sino también, en sentido inverso a la averiguación de los números de teléfono y/o **datos identificativos de cualquier otro medio de comunicación,** es decir a la identificación de dispositivos concretos o de un medio de comunicación cuando ello fuera necesario para el ejercicio de las funciones encomendadas al Ministerio Fiscal o a la Policía Judicial en el marco de la investigación criminal.

El precepto que nos ocupa ha de interpretarse, a su vez, en relación con el artículo 588 ter j del mismo texto legal relativo a la incorporación al proceso de los datos obrantes en archivos automatizados de los prestadores de servicios según el cual:

1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos 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.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

En la aplicación de este nuevo precepto de la Ley de Enjuiciamiento Criminal se han suscitado problemas ante la negativa de algunos de los operadores de comunicaciones radicados en España a facilitar directamente y sin autorización judicial, y por tanto con base en el artículo 588 ter m), el dato IMEI correspondiente a un determinado dispositivo móvil o el de número o números IMSI que aparecen asociados a un dispositivo electrónico –y por tanto a un IMEI concreto- en un periodo delimitado de tiempo y ello aun cuando dicha información se solicite de forma aislada y por tanto desligada de cualquier otra información relacionada con posibles procesos de comunicación mantenidos desde el terminal especifico en el referido espacio temporal. La cuestión se suscita a propósito de algunas investigaciones relacionadas con delitos contra la propiedad con ocasión de los cuales, bien sea de forma exclusiva o conjuntamente con efectos de otra naturaleza, las víctimas fueron despojadas de sus aparatos de telefonía móvil. En muchos de estos supuestos, para el esclarecimiento del hecho y la identificación de sus autores, puede resultar de especial interés conocer la tarjeta SIM –o número IMSI- que ha sido utilizada en el terminal físico sustraído en las horas o días inmediatamente posteriores a la ejecución de la actividad ilícita, con independencia de cuales o cuantas hayan sido las comunicaciones concretas que se hayan realizado desde el mismo.

Antes de explicar las razones que aducen las compañías para negarse a facilitar dicha información y analizar el fundamento de las mismas, resulta conveniente realizar un breve estudio del significado de estos conceptos telemáticos y de la relación que los mismos guardan con el desarrollo y la identificación de procesos de comunicación determinados. Con el fin de clarificar dichos extremos, esta Unidad Central del Área de Especialización en Criminalidad Informática ha recabado de los Gabinetes Técnicos del Cuerpo Nacional de Policía y de la Guardia Civil sendos estudios que se adjuntan como anexos, y de los que se extraen las siguientes conclusiones:

* Un dispositivo de comunicaciones móviles celulares -lo que coloquialmente llamamos teléfono móvil- se compone de dos elementos: a) el terminal físico o equipo electrónico móvil y b) el módulo de identificación de usuario, conocido como tarjeta SIM *(Subscriber Identity Module*). Esta tarjeta SIM es intercambiable entre los diferentes terminales móviles y contiene en su chip digital la información necesaria para identificar y autenticar al abonado, incluido el número IMSI

*El **IMEI** *(International Mobile Equipement Identity*) es un código que identifica inequívocamente a un determinado dispositivo móvil (terminal físico). Este número se incorpora obligatoriamente por el fabricante al terminal y ha de ser inalterable desde su producción, por

lo que ha de ser resistente a la manipulación que pueda llevarse a cabo por cualquier medio. Identifica por tanto al equipo físico respecto a cualquier otro aparato con independencia del abonado concreto que esté haciendo uso del terminal en cada momento.

*El **IMSI** *(International Mobile Suscriber Identity*) es el código que identifica internacionalmente al abonado de una línea de comunicación móvil. Se trata de un código único que se integra en una tarjeta SIM la cual tiene como destino insertarse en un dispositivo móvil concreto (terminal físico). A partir del IMSI se asigna al usuario de esa tarjeta un número de abonado o MSISDN (*Moblile Station Integrated Services Digital Network*) que conocemos como número comercial. Se trata por tanto del código que permite al abonado el acceso a los servicios contratados y al proveedor el control de la información necesaria para realizar la correspondiente facturación.

El IMSI se integra por una serie alfanumérica de cuya lectura aislada no se obtienen directamente datos de identificación de persona alguna pero que una vez contrastada con los archivos, registros y bases de datos de los operadores permite obtener información de interés y en particular, el número telefónico comercial del abonado, su identidad y otros datos asociados.

El IMSI es, por tanto, el código de identificación por excelencia y es el elemento que se utiliza en todo tipo de conexiones entre el dispositivo móvil y la red, estén o no vinculadas a procesos de comunicación concretos. Así, por ejemplo, el IMSI queda registrado en las redes GSM y UMTS y en consecuencia localizado y controlado por la compañía operadora como consecuencia de la mera puesta en funcionamiento –o encendido- del dispositivo electrónico correspondiente. En cuanto al código IMEI, identificador del dispositivo electrónico, su control queda al arbitrio del operador aunque generalmente suele efectuarse la revisión de este código cada vez que el dispositivo se conecta a la red ya que constituye el mecanismo de seguridad establecido internacionalmente para poder rechazar las comunicaciones que se realizan desde terminales prohibidos, no compatibles con la red o que se encuentran sujetos a control por haber sido sustraídos o ser objeto de comercio ilícito.

*La tarjeta SIM es facilitada por la compañía proveedora del servicio de comunicaciones a aquellos clientes que con ella hayan contratado el servicio como abonados y en la misma se incluye toda la información antes indicada, incluido el número IMSI. Por el contrario, el terminal móvil puede ser adquirido en cualquier establecimiento del sector o puede también ser facilitado por el propio proveedor de comunicaciones. En consecuencia, las operadoras disponen, en sus bases de datos de clientes y de facturación, de información sobre los datos personales del cliente, la tarjeta SIM y el número IMSI que le identifica como tal abonado. Igualmente dispondrán de información sobre el IMEI concreto (identificación del terminal) al que -en principio- se asoció el uso de la tarjeta en todos aquellos casos en que la misma compañía haya proporcionado a su cliente ambos elementos, es decir no solo la tarjeta SIM sino también el dispositivo físico.

Pues bien, como se señalaba anteriormente, algunas operadoras españolas se han negado a facilitar a los cuerpos policiales la información relativa a la vinculación entre un dispositivo físico (identificado por el IMEI) y un número IMSI (integrado en la tarjeta SIM). En definitiva, consideran que no puede informarse, sin previa autorización judicial, ni a dichos agentes ni

tampoco al Ministerio Fiscal acerca de cuál es la tarjeta SIM concreta con que está funcionando un determinado terminal de telefonía móvil o, en sentido contrario, qué móvil concreto está siendo utilizado para el funcionamiento de una tarjeta SIM determinada y ello aun cuando la petición no incluya solicitud alguna acerca de hipotéticas comunicaciones que hayan podido ser mantenidas desde ese terminal

Argumentan las operadoras para justificar su negativa que sus bases de datos de clientes solo contienen esa información en el supuesto, antes indicado, de que la propia compañía haya facilitado conjuntamente ambos elementos al abonado y además en referencia exclusiva al momento de la adquisición del terminal y la tarjeta. En los demás casos, la localización y facilitación de la información necesaria para vincular la utilización de la tarjeta SIM a un dispositivo determinado ha de hacerse a partir de los registros derivados de las conexiones con la red efectuadas desde dicho dispositivo, momento en el que el operador puede captar no solamente el IMSI de la tarjeta sino también el IMEI identificativo del terminal físico utilizado como soporte. Por ello, según se expone por los operadores, para atender la indicada solicitud de los cuerpos policiales -o, en su caso, del Ministerio Fiscal- sería imprescindible llevar a cabo la oportuna búsqueda en las bases de datos en que se almacena el tráfico cursado por dicha línea móvil, siendo necesario para el acceso a las mismas la autorización judicial previa que exige la Ley 25/2007 de 18 de octubre sobre conservación de datos de las comunicaciones electrónicas.

Planteada en estos términos la cuestión debatida, resulta necesario aclarar si la información que se demanda en estos casos puede considerarse como datos de abonados (*subscriber information*) o por el contrario, se trata de datos de tráfico vinculados a una comunicación, pues tal circunstancia va a resultar determinante a los efectos de valorar el régimen jurídico a que se somete la obtención de los mismos. Efectivamente, los datos relacionados con las comunicaciones electrónicas se suelen clasificar en tres categorías distintas: datos de contenido, datos de tráfico y datos sobre abonados. Dejando de lado los datos de contenido que carecen de interés a los efectos que nos ocupan, la delimitación entre datos de abonado y datos de tráfico ha de hacerse teniendo en cuenta los criterios internacionales que se han ido fijando al respecto en los últimos años. Así, la Convención sobre Ciberdelincuencia del Consejo de Europa[1] se refiere su artículo 18.3 a los datos relativos a abonados en los siguientes términos:

Art 18.3.-*A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:*

a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

[1] Esta Convención fue publicada en Budapest el 23 de Noviembre de 2001 y ratificada por España en instrumento publicado el 20 de mayo de 2010

b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios

c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

El informe preparatorio de la Convención de Budapest aclara con más detalle alguno de estos conceptos, y concretamente el apartado a) del citado precepto, al explicar que por disposiciones técnicas para la utilización del servicio han de entenderse todas las medidas adoptadas para hacer posible que un abonado disfrute del servicio de comunicación, incluyéndose entre *ellas la reserva de un número o una dirección técnica (número de teléfono, dirección de un sitio web o nombre de dominio, dirección de correo electrónico etc), así como también la provisión y el registro de los equipos de comunicación utilizados, tales como los teléfonos, las centrales telefónicas o las redes de área local.*

De ello puede concluirse que los códigos de identificación IMEI e IMSI, cuyo objeto y finalidad es la identificación respectivamente del terminal físico y del usuario, han de considerarse incluidos en este concepto de datos sobre abonados, siempre que la solicitud/facilitación de los mismos se haga como dato independiente y aislado o desvinculado de cualquier información sobre los procesos comunicativos en que dichas numeraciones hayan podido ser utilizadas.

Ese es sin duda el criterio adoptado por el legislador español, que en el nuevo artículo 588 ter l de la Ley de Enjuiciamiento Criminal y recogiendo de esta forma la doctrina jurisprudencial fijada al respecto (SSTS nº 246/2014 de 2 de abril y nº 481/2016 de 2 de junio, SSTS nº 256/2017 de 6 de abril entre otras muchas) se refiere expresamente a las numeraciones IMEI e IMSI como códigos de identificación o etiquetas técnicas de los aparatos de comunicación al establecer que, precisamente por tener esa condición –meramente identificativa-, pueden ser captados directamente por los agentes de Policía Judicial en el curso de sus investigaciones sin precisar para ello de autorización judicial.

Por otra parte, si analizamos la naturaleza de los códigos IMEI e IMSI a la luz de la delimitación que se viene efectuando sobre lo que ha de entenderse por datos de tráfico, se obtiene la misma conclusión. Efectivamente, la Convención de Budapest define este concepto en su artículo 1 d) en los siguientes términos:

Art 1 d.-por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Nótese que la circunstancia que cualifica como dato de tráfico una determinada información sobre origen, ruta, hora, fecha, tamaño, duración o servicio utilizado es que la misma se solicita/facilita en referencia a una comunicación o comunicaciones concretas. Se explica muy bien en los trabajos preparatorios de la Convención del Budapest al indicar que son los datos *generados por los ordenadores en la cadena de comunicación con el fin de encaminar una comunicación desde su punto de origen hasta su destino. Por tanto, son datos auxiliares a la*

comunicación misma. Por ello considera que constituyen una categoría separada de datos informáticos sujeta a un régimen jurídico específico.

En plena coherencia con este mismo planteamiento el legislador español al regular, en el artículo 588 ter j LECrim, el acceso al proceso penal de los datos de tráfico o asociados conservados por los operadores de comunicaciones limita la exigencia de autorización judicial a aquellos datos que se encuentren **vinculados a un proceso de comunicación**, no así a los restantes para los que no es imprescindible este requisito. Entre estos últimos datos informáticos han de incluirse, sin duda, los que permiten identificar titulares, terminales o dispositivos de conectividad, cuya obtención se ha estimado oportuno someter a una regulación específica en el artículo 588 ter m) del mismo texto legal en el que, de conformidad con lo anteriormente indicado, se establece que dicha información puede obtenerse directamente de los operadores o prestadores de servicio por el Ministerio Fiscal o la Policía Judicial, sin necesidad de intervención judicial

En consecuencia, es evidente que los códigos IMEI e IMSI cuando son solicitados/facilitados de forma autónoma, es decir, como datos aislados y al margen de su efectiva utilización en procesos de comunicación concretos, no pueden catalogarse como datos de tráfico, sino únicamente como lo que son: códigos identificativos del terminal físico (IMEI) o del abonado concreto (IMSI) y es igualmente evidente que la vinculación de ambas informaciones únicamente sirve para la individualización completa del equipo móvil, en sus dos componentes, sin que ello suponga revelar dato alguno sobre el uso de ese dispositivo. Por consiguiente, la afectación a derechos fundamentales derivada de la obtención de este tipo de información es prácticamente imperceptible.

Este criterio se encuentra plenamente avalado, a nuestro entender, por la reciente Sentencia dictada en fecha 2 de octubre de 2018 por el Tribunal de Justicia de la Unión Europea en el asunto C-207/2016. Ministerio Fiscal, en la que se responde a una cuestión prejudicial planteada por la Audiencia Provincial de Tarragona en un supuesto muy similar al que es objeto de análisis en este Dictamen. El tema objeto de debate en este caso fue, precisamente, el nivel de injerencia que tiene, en derechos fundamentales, la obtención de información acerca de la titularidad de la tarjeta SIM utilizada en un determinado móvil previamente sustraído. Al respecto recuerda el Tribunal de Justicia de la UE que dicha información solo permite vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM, añadiendo a continuación que sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de su localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período temporal concreto. Esta situación lleva al TJUE a considerar que las informaciones reclamadas en este supuesto no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados, por lo que la obtención de las mismos no puede calificarse de injerencia «grave» en los derechos fundamentales de los individuos cuyos datos se ven afectados. (parágrafos 59 a 61 de la mencionada resolución).

Es por ello que el régimen aplicable a la obtención de esta información ha de ser el establecido en el artículo 588 ter m) de la LECrim, conclusión que resulta corroborada por las propias manifestaciones que recoge el legislador español en el Preámbulo de la LO 13/2015 al indicar que el citado precepto tiene por objeto regular *la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal o la Policía Judicial en el ejercicio de sus funciones sin necesidad de autorización judicial.*

Esta nueva previsión legal, obliga a una reinterpretación de los criterios que hasta el momento se venían manteniendo respecto a la cuestión objeto de análisis. Previamente a la reciente reforma procesal, como ya se ha indicado, se encontraba plenamente consolidada la doctrina jurisprudencial según la cual *queda extramuros del ámbito del secreto de las comunicaciones protegido constitucionalmente el conocimiento del IMSI o IMEI de los teléfonos*, por lo que su captura no precisa de autorización judicial (STS 481/2016 de 2 de junio y 551/2016 de 22 de junio, STS nº 256/2017 de 6 de abril (entre otras muchas) Es más, en relación con el número IMSI nuestra jurisprudencia ha indicado también que se trata de un dato enmarcado en el ámbito de protección *de la intimidad de los ciudadanos frente a la utilización de la informática* que otorga el art 18.4 de la CE (por todas STS 249/2008 de 20 de mayo) si bien matiza que el mismo no se encuentra incluido en el núcleo duro de la privacidad protegido especialmente por el art 7.2 LO 15/1999. Sobre la base de esta doctrina y complementando la misma, nuestros Tribunales han venido entendiendo -hasta el momento- que la solicitud a los operadores de comunicación de los datos de identificación del titular o de su número de abonado, a partir de esas numeraciones IMEI e IMSI, exigía autorización judicial porque la obtención de esa información aun no estando sometida al régimen de exclusiva reserva judicial –por no afectar al secreto de las comunicaciones ni tratarse de un dato especialmente protegido- precisaba de ese requisito por disponerlo así la Ley 25/2007 de 18 de octubre *sobre conservación de datos de las comunicaciones electrónicas y redes públicas de comunicación*. Sin embargo, es evidente que con la incorporación del nuevo artículo 588 ter m) en la Ley de Enjuiciamiento Criminal, el legislador da un nuevo enfoque a esta cuestión al prever expresamente que la identificación de titulares o terminales o dispositivos de conectividad pueda solicitarse directamente, en las condiciones indicadas, a los prestadores de servicios de comunicaciones, tanto por parte de la Policía Judicial como del Ministerio Fiscal.

Esta solución no es en modo alguno contradictoria con la vigencia de los artículos 1 y 3 de la Ley 25/2007 en los que se establece la necesidad de autorización judicial cuando lo que se pretende es la identificación de los equipos de comunicación específicos que, como emisor y receptor, han intervenido en una concreta comunicación. Efectivamente, el Preámbulo de la citada disposición legal lo señala con claridad al indicar que los datos que han de conservarse en aplicación de dicha norma son los necesarios para identificar el origen y destino de una comunicación, su hora, fecha y duración y el tipo de servicio y equipo utilizado por los usuarios con ocasión de la misma. Por ello la información almacenada y susceptible de ser reclamada/facilitada al amparo de esta ley no puede considerarse simplemente como información sobre abonados, sino que su naturaleza, en esas circunstancias, es más próxima al concepto de datos de tráfico que anteriormente ha sido explicado.

Catalogados, por tanto, los códigos IMEI e IMSI como datos de abonados, el acceso a los mismos queda sometido al régimen jurídico establecido en el artículo 588 ter m), por lo que los operadores o prestadores de servicios de telecomunicaciones o de la sociedad de la información han de atender las solicitudes de identificación que, al respecto, se cursen directamente por parte del Ministerio Fiscal o de la Policía Judicial con ocasión de una investigación criminal. Tal cuestión no suscita duda alguna cuando dicha información se encuentra almacenada en las bases de datos de clientes o de facturación de dichas entidades. Sin embargo, y como se ha indicado, algunos operadores consideran que cuando la información solicitada se encuentre almacenada conjuntamente con los datos de tráfico conservados en aplicación de la citada Ley 25/2007 -básicamente en los supuestos en los que se demanda la tarjeta SIM (o número IMSI) asociados a un determinado IMEI en un especifico periodo temporal- el acceso a dicha información exige autorización judicial, porque su obtención se encuentra protegida por las garantías establecidas en la mencionada disposición legal.

En relación con ello ha de recordarse, en primer término, que el registro del código IMSI que aparece vinculado a un determinado terminal físico identificado por el IMEI, puede obtenerse por la mera puesta en funcionamiento –conexión a la red- del dispositivo móvil, sin necesidad de que se produzca un proceso de comunicación interpersonal, por lo que la obtención de dicha información queda al margen de las circunstancias concretas en que se lleven a efecto ulteriores procesos comunicativos. Pero, además, la forma en que los operadores de comunicaciones decidan controlar/almacenar estos datos no puede suponer, en ningún caso, una modificación del régimen jurídico aplicable a los mismos y, en consecuencia, de las condiciones para su obtención hasta el punto de que esa circunstancia determine la necesidad de la previa autorización judicial.

Al respecto, no ha de olvidarse que los operadores de comunicaciones no precisan de autorización judicial para acceder a la información por ellos conservada, y cuya custodia les compete, sino que, tal autorización previa únicamente es exigible e ineludible, de conformidad con el artículo 1º de la mencionada ley 25/2007, para *la cesión de dichos datos a los agentes facultados* por parte de los operadores de comunicaciones. Es decir, la autorización judicial no tiene por objeto permitir la consulta de las bases de datos a quienes son responsables del almacenaje y conservación de la información sino garantizar que la entrega a terceros de los datos protegidos solo se hace en aquellos casos en que el órgano judicial competente lo estima oportuno y en las condiciones en que por el mismo se acuerde. Desde ese planteamiento poco importa, a los efectos que nos ocupan, dónde se encuentren almacenados los datos demandados sino únicamente cuál es su carácter y contenido a los efectos de valorar si su entrega por los operadores de comunicación o proveedores de servicios puede hacerse directamente a los solicitantes o exige autorización judicial.

En base a este razonamiento se adoptan las siguientes conclusiones:

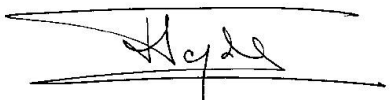
A) Los códigos de identificación IMEI e IMSI, cuyo objeto y finalidad es la identificación respectivamente del terminal físico y del usuario del servicio de comunicación, tienen la consideración de *datos sobre abonados* siempre que la solicitud/facilitación de los mismos se haga como dato independiente y aislado o desvinculado de cualquier otra

información sobre los procesos comunicativos en que dichas numeraciones hayan podido ser utilizadas.

B) La cesión de dichos códigos de identificación, bien sea de forma aislada bien vinculados entre sí, por parte de los operadores de comunicaciones o proveedores de servicios, en las circunstancias antedichas, se encuentra sometida al régimen jurídico establecido por el artículo 588 ter m de la Ley de Enjuiciamiento Criminal y por tanto podrán ser solicitados directamente por el Ministerio Fiscal o la Policía Judicial en el ejercicio de sus funciones de investigación criminal.

C) Los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información que, previo apercibimiento, incumplan los requerimientos de información sobre dichos códigos de identificación en las antedichas circunstancias podrían incurrir en delito desobediencia de conformidad con lo establecido en el citado artículo 588 ter m) Ley de Enjuiciamiento Criminal.

Madrid 5 de marzo de 2019



Elvira Tejada de la Fuente

LA FISCAL DE SALA COORDINADORA