N/REF: 0030/2021

La consulta se centra en la adecuación al marco jurídico vigente respecto del acceso por parte de las Fuerzas y Cuerpos de Seguridad del Estado (FCS en lo sucesivo), a la información de la que disponen las Operadoras de Telecomunicaciones (las operadoras en lo sucesivo) derivado de los servicios que prestan y de las posibilidades de que conforme a la ley puedan mejorar el sistema para la lucha contra este tipo de estafas.

SIM Swapping es el término coloquial a través del que se conoce este tipo de estafa que consiste, principalmente, en que un tercero ajeno al titular de la tarjeta SIM, solicita a la operadora correspondiente un duplicado de dicha tarjeta SIM (que supone la anulación de la anterior tarjeta SIM), para recibir en dicho duplicado los mensajes de texto SMS que la entidad bancaria envía a sus clientes como medida de seguridad para confirmar determinadas operaciones bancarias.

Este tipo de estafa requiere que previamente el tercero haya conseguido hacerse con las credenciales de la víctima para acceder y autenticarse en el servicio de banca electrónica.

Una vez que el tercero tiene acceso a los servicios de banca electrónica y a la tarjeta SIM de la víctima (tarjeta duplicada), puede operar con total libertad para realizar movimientos en las cuentas corrientes y otros productos financieros de aquella, pues la realización de cualquier operación pasa por el envío de un mensaje SMS de confirmación a la línea de teléfono que el afectado haya proporcionado a la entidad bancaria a esos efectos, y que en este caso, ha sido *duplicada* y está en poder de dicho tercero.

Por lo tanto, puede afirmarse que el tratamiento objeto de análisis debe tener en cuenta el estadio inicial que sucede en la entidad bancaria cuando el tercero *se hace con las credenciales* de acceso *y autenticación* de la víctima, en un segundo momento, la suplantación de la identidad ante la operadora para acceder al duplicado de la tarjeta SIM y el ultimo estadio de este tratamiento es la comunicación a las FCS y al Ministerio Fiscal para su investigación.

I

Existe en la actualidad un Grupo de Trabajo constituido entre los agentes facultados (artículo 6.2 de Ley 25/2007, de 18 de octubre, de

conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, o LCDT) y las operadoras, (GT Agentes facultados-Operadoras) para dar cumplimiento a las solicitudes de información referidos a datos sujetos a mandamiento judicial (artículo 3 LCDT), entre cuyas cuestiones se aborda la operativa sobre la entrega de dicha información.

A estos efectos, se utiliza un sistema general de intercambio de información SIGMA que supone el acceso prácticamente inmediato por parte de los agentes facultados a dicha información, del que se pueden distinguir dos subtipos o clases, automatizado (XML) y otro semiautomatizado (VPN-SFTP), en el que las operadoras proporcionan a los agentes facultados “información estructurada” y que se concreta a aquella a la que se refiere el citado artículo 3 LCDT.

Ahora bien, en la investigación policial relacionada con este tipo de estafa, cobran especial importancia los datos referidos a la fecha y hora y forma de la activación del duplicado de una tarjeta SIM, es decir, qué tipo de canal se utilizó, si fue online o si fue presencial/físico y la ubicación desde la que se llevó a cabo, en caso de realizarse por un canal presencial. A lo que hay que añadir, cualquier documentación sobre la que se apoyó la solicitud del duplicado.

Sin embargo, en relación con el sistema de intercambio de información, toda esta se considera como “información no estructurada” y supone que el operador deba realizar la consulta “manual” afectando negativamente a la rapidez y efectividad de investigaciones en las que son esenciales dichos datos.

En relación con este aspecto la Secretaria de Estado de Seguridad en su informe aportado en las reuniones del GT1, indica lo siguiente “*Los delincuentes conocen estas dilaciones y aprovechan para cometer este tipo de hechos en las fechas y horas en que a los usuarios de banca y telefonía les es más complicado contactar con los servicios de atención al cliente de la banca y los operadores por no funcionar al 100%, como fines de semana, final de la tarde o noche, festivos y puentes; resultando que cuando se presenta denuncia en dependencia policial, a diferencia de las consultas sobre titularidad telefónica, los agentes no pueden conocer dichos datos con inmediatez, resultado perjudicado al ciudadano y a la propia banca y operadores, por la afección económica o a su prestigio*”

Teniendo en cuenta lo anterior, las dudas que se plantean en el seno del GT1 es si dicha información que se estima necesaria para la investigación

de este tipo de estafas, está bajo la protección de la Ley 25/2007 de 18 de Octubre, es decir, si pueden ser considerados *datos de tráfico vinculados a un proceso de comunicación*, y en caso afirmativo si la aplicación de la citada ley cumple con las exigencias del principio de proporcionalidad según la STJUE de 8 de abril de 2014 (Asunto C-293/2012) o si por el contrario son datos de referidos *a la "titularidad" del servicio, es decir, datos de abonado* y por tanto sometidos al régimen de acceso que prevé el articulo 588 ter m de la Ley de Enjuiciamiento Criminal (LECrim), y en su caso al Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, o la Directiva (UE) 2016/680. Puesto que, dependiendo del régimen jurídico aplicable, será necesario entonces autorización judicial para poder acceder a la información que las FCS y el Ministerio Fiscal entiende necesaria para investigar y perseguir este tipo de delitos.

Por lo tanto, teniendo en cuenta que la cuestión principal objeto de análisis, es si para el acceso a determinada información va a ser necesaria autorización judicial o no, por entender que se aplica una norma u otra, y en segundo término o consecuencia de lo anterior, el modo o manera en que las operadoras almacenan los datos de tráfico del servicio de telecomunicaciones, conviene adelantar ya que es una cuestión ajena a la competencia de esta Agencia Española de Protección de Datos, y que el presente informe se limita a analizar el tipo de datos objeto de tratamiento, y de acuerdo con la normativa aplicable proponer las alternativas que entiende ajustada a Derecho, sin perjuicio del mejor criterio de aquellos organismos o instituciones con competencia especifica en la materia, como podrían ser el Consejo General del Poder Judicial o los órganos de la jurisdicción ordinaria o Constitucional que deba conocer de estos asuntos.

II

Teniendo en cuenta lo anterior, procede establecer la siguiente diferenciación referida a los datos relacionados con **el proceso de identificación del abonado para solicitar el duplicado de la SIM,** que es la información cuyo acceso considera fundamental las FCS para perseguir este tipo de delitos con celeridad y eficacia:

> Información relacionada con la solicitud: (i) tipo de canal utilizado, si es presencial, información sobre la ubicación física del distribuidor, (ii) fecha y hora de la solicitud, cuándo y cómo verificó la operadora la identidad del solicitante, y en qué lugar, así como (iii) la documentación aportada para la tramitación de la solicitud.

Información relacionada con la activación de la "nueva" SIM: (iv) fecha y hora en la que se produce la activación y su ubicación, así como otra información que puede resultar relevante: el IMEI del dispositivo con el que se activa la SIM duplicada (el IMEI lo tienen todos los dispositivos *asignado de fábrica* y sirve para identificar unívocamente un dispositivo), o el IMSI que se está utilizando en un determinado dispositivo ,o dicho de otro modo el IMSI que se relaciona con un determinado IMEI.

Conviene aclarar, en primer lugar, que el IMSI se integra en la tarjeta SIM, y sirve para identificar internacionalmente al abonado, y a partir del cual se asigna un MSISDN que se conoce como número comercial, conocido coloquialmente como el número de teléfono. Y, en segundo lugar, debe tenerse en cuenta que la tarjeta SIM contiene una programación que, una vez introducido el PIN permite la búsqueda de redes GSM y UMTS y trata de conectarse en una de ellas. Cuando se ha conectado a la red, el teléfono (IMSI y IMEI) queda registrado y estará disponible para usar los servicios contratados.

Por lo tanto, el IMSI aparecerá en todas las conexiones entre el dispositivo y la red, con independencia del proceso comunicativo.

Respecto del IMEI, como se ha indicado antes, sirve para identificar unívocamente el dispositivo en la red, y también se usa para contrastarlo con la base de datos EIR (Equipment Identity Register) a los efectos de posibilitar la recepción y emisión de llamadas, pues en dicha base de datos se incluyen aquellos IMEI de dispositivos autorizados para realizar y recibir llamadas y aquellos que no, ya sea porque corresponde a equipos robados o utilizados de forma ilegal o porque su acceso al sistema podrían producir graves problemas técnicos; por lo tanto, no pueden realizar ni recibir llamadas.

La consecuencia del funcionamiento del sistema descrito es que cuando se produce esa conexión entre el dispositivo y la red, las operadoras captan no solo el IMSI, sino también el IMEI del dispositivo. Es decir, las operadoras de red conocen esa vinculación entre el IMSI y el IMEI.

En este sentido, procede citar en primer lugar, el Informe de 19/10/2016 de la Comisión Nacional los Mercados y la Competencia (CNMC) indica que:

"*Respecto a la cuestión de la vinculación de un IMEI con los datos de un suscriptor (IMSI, MSISDN), aun no existiendo un conocimiento de antemano por parte del operador de qué IMEI utiliza un suscriptor (un usuario tiene la libertad de utilizar los equipos que desee*

sin previa información al operador), cuando éste realiza un registro en la red móvil o realiza una llamada, el operador sí tiene conocimiento de que un determinado equipo identificado con un IMEI se ha registrado o utiliza la red móvil utilizando un determinado IMSI."

En segundo lugar, procede citar lo indicado en el anexo I del Dictamen 1/19 de la Unidad 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 (Dictamen 1/19 en lo sucesivo), que analiza qué informacion captan las operadoras con la conexión a la red de un dispositivo móvil:

En relación con todo lo anterior, la instrucción técnica del estándar correspondiente 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, excepto en aquellos que se produzcan para cerrar la conexión. 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 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 .*

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.

Según afirman las FCS y la Fiscalía en sus informes y dictámenes aportados al presente GT1, resulta necesario en muchas ocasiones conocer **la vinculación entre un IMEI y el IMSI**. Es decir, qué tarjeta SIM (IMSI) está siendo utilizada en un determinado terminal físico (IMEI) y a la inversa, que móvil concreto (IMEI) está siendo utilizado para la puesta en funcionamiento de una determinada SIM.

En el primer supuesto, se conoce el IMEI, el dispositivo físico, y se quiere conocer el IMSI (que está integrado en la SIM); y en el segundo supuesto, se conoce el IMSI y se quiere saber qué dispositivo la utiliza, es decir, el IMEI.

Pues bien, en este escenario conviene analizar la información que almacenan y manejan las operadoras en relación con dicha vinculación, frente a lo que caben, con carácter general dos situaciones:

A) La primera es aquella en la que la operadora proporciona la tarjeta SIM, que como se ha indicado contiene también el IMSI, y que va a prestar el servicio de telecomunicaciones, y también proporciona el dispositivo físico, que contiene el IMEI. En términos coloquiales la compañía *le da al usuario tanto el móvil, como la tarjeta SIM*.

En estos casos, la operadora tendrá la información sobre el cliente y el servicio (identificación, cuenta bancaria, domicilio, y comunicaciones realizadas para la correspondiente facturación, etc.,) y en lo que aquí interesa, dispondrá del IMEI del dispositivo al que se asoció la tarjeta SIM (IMSI). Es decir, tendrá toda la información referida

a la “vinculación entre un IMEI y el IMSI” a la que antes se ha hecho referencia.

B) La segunda situación es aquella en la que la operadora proporciona la tarjeta SIM, pero sin embargo, no proporciona el dispositivo físico, pues la tarjeta se puede utilizar en cualquier terminal compatible vendido por otra operadora o por otra entidad incluso ajena a los servicios de telecomunicaciones, y por tanto, a priori, la operadora que recibe la solicitud de las FCS o de la Fiscalía, desconoce el IMEI relativo al móvil en el que se está usando la citada tarjeta, por no constar en su base de datos de clientes, como si sucede en el primer caso.

Es esta segunda situación la que, en la práctica, según afirman las FCS está planteando problemas por la reticencia de las operadoras a facilitar dicha información referida a la vinculación entre un IMEI y el IMSI.

En efecto, según consta en el *Dictamen 1/19*, afirman las operadoras que para localizar y facilitar esa información 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*.”

Frente a ello, el referido Dictamen 1/19, tras realizar un exhaustivo análisis sobre la aplicación del artículo 588 ter m) de la LECrim y la inaplicación de la Ley 25/2007 de 18 de octubre, a este tipo de información, indica que “*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*.”(…) *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. (…)

Por otra parte, la Dirección General de Telecomunicaciones en los informes aportados en el seno del GT, entiende conforme a la jurisprudencia del TJUE que la legislación nacional permita la retención preventiva de datos relacionados con la identidad civil con el fin de salvaguardar la seguridad nacional, combatir la delincuencia y salvaguardar la seguridad pública y por tanto, que la conservación de datos relacionados con la identidad civil de los usuarios de los sistemas de comunicaciones electrónicas puede ser general sin que se exija a los Estados miembros la limitación del período de conservación.

Añade que, sin embargo, la Ley 25/2007 de 18 de octubre *no contiene ninguna norma clara y precisa sobre el alcance y la aplicación de la medida en relación con el caso de duplicado de tarjetas SIM y, por tanto, difícilmente cumpliría el criterio de proporcionalidad que, según el Tribunal de Justicia exige que la norma nacional sea una norma específica de la legislación nacional.*

III

Con carácter previo debe indicarse que la Ley 25/2007 de 18 de octubre es fruto de la transposición de la *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 y por la que se modifica la Directiva 2002/58/CE*, **que fue anulada por la Sentencia del TJUE de 8 de abril de 2014**, Asunto C-293/2012, por considerar que *el legislador de la Unión sobrepasó los límites*

que exige el respeto del ***principio de proporcionalidad*** *en relación con los artículos 7, 8 y 52, apartado 1, de la Carta (LCEur 2000, 3480)* fundamentalmente en base a las siguientes consideraciones:

Trata de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves. (apartados 57 y 58)

No establece ningún criterio objetivo que permita garantizar que las autoridades nacionales competentes puedan acceder únicamente a los datos y puedan utilizarlos para prevenir, detectar o reprimir penalmente delitos que, por la magnitud y la gravedad de la injerencia en los derechos fundamentales en cuestión, puedan considerarse suficientemente graves para justificar tal injerencia, sino que:

a. Hace una remisión general a los «delitos graves» definidos por cada Estado miembro en su ordenamiento jurídico interno. (apartado 59)

b. no define las condiciones materiales y procesales en las que las autoridades nacionales competentes pueden tener acceso a los datos y utilizarlos posteriormente. (apartado 60)

c. el acceso a los datos no se supedita al control previo de un órgano jurisdiccional o de un organismo administrativo autónomo. (apartado 62)

Establece un período de conservación de los datos que oscila entre seis y veinticuatro meses, sin que se determina una distinción entre las categorías de datos en función de las personas afectadas o de la posible utilidad de los datos con respecto al objetivo perseguido. (apartado 63 y 64)

No establece garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos de los datos. (apartado 66)

No obliga a que los datos se conserven en el territorio de la Unión, por lo que no se garantiza plenamente el control del cumplimiento de los requisitos de protección y de seguridad. (apartado 68)

No obstante, lo anterior, la Ley 25/2007 de 18 de octubre, sigue vigente y es de plena aplicación en tanto que la invalidez de la Directiva no debe trasladarse, *ipso iure*, a la norma de transposición, siendo los órganos

competentes para su aplicación, los que deberán de interpretar su adecuación al derecho comunitario y/o nacional y en especial al **principio de proporcionalidad** que es el que en palabras del TSJUE se ha vulnerado.

Además la propia Ley 57/2007, de 18 de octubre, a diferencia de la Directiva anulada, establece, precisamente, **el control judicial sobre el acceso a la información que es objeto de protección**, por lo que "juicio de proporcionalidad" se presume intrínseco en la autorización judicial de que se trate para el caso concreto -tal como se extrae de los Capítulos IV y V, Título VIII del Libro II de la LECrim-, y por tanto, ya se habrá valorado el respeto o la injerencia necesaria en el derecho a la protección de datos y a la vida privada de los afectados.

Sobre la "validez de la Ley 25/2007" tras la anulación de la Directiva, el **Tribunal Supremo** en Sentencia **núm. 727/2020 de 23 de marzo,** indica:

> *A este fin debemos hacer una primera observación. El hecho de que se haya declarado la invalidez de la Directiva 2006/24/CE no significa que las leyes nacionales de trasposición que la desarrollaron en cada país sigan la misma suerte.*
>
> *Una Directiva es un instrumento de armonización de las legislaciones nacionales pero que admite márgenes de discrecionalidad. Tan es así que en relación con la conservación de datos las legislaciones de cada Estado miembro evidencian notorias diferencias. De ahí, que una vez vigente la norma nacional, si es respetuosa con el derecho de la Unión, tiene autonomía respecto de la Directiva que justifica su nacimiento y sólo puede ser derogada por una norma posterior. Ciertamente las sentencias del Tribunal de Justicia de la Unión son vinculantes, pero en lo que atañe a este caso, las sentencias que se acaban de citar no conllevan de forma ineludible la nulidad de la Ley 25/2007, sino que obligan a analizar si el régimen de conservación de datos en España, cuya regulación no se limita a la ley citada, es conforme con el derecho de la Unión.*
>
> *Resulta obligada una segunda observación. En este momento la Unión Europea, una vez anulada la Directiva 2006/24/CE, carece de un instrumento de armonización de las legislaciones nacionales. La ausencia de una norma comunitaria obliga a centrar la atención en la doctrina del TJUE y no podemos dejar de destacar que cada nueva sentencia del alto tribunal, tal y como hemos tratado de resumir anteriormente, añade matices, establece excepciones, diseña nuevos*

requisitos y modulaciones, estableciendo doctrinas que adicionan y acumulan conceptos normativos que acrecientan su complejidad jurídica. Y tan es así que el propio TJUE en buena medida ha desplazado el problema de la licitud de la norma a la validez probatoria de la información obtenida a partir de los datos conservados por exigencias de las normativas nacionales, lo que, a nuestro juicio, evidencia que el alto tribunal es consciente de la complejidad de la situación creada como consecuencia de su propia doctrina y, sobre todo, de la ausencia de un marco normativo que dote de la necesaria seguridad jurídica a esta compleja materia.

Según venimos comentando, en España esta materia se regula por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuyo objeto declarado en la Exposición de Motivos, se promulgó con la finalidad de trasponer al derecho interno la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo.

Esta Ley ha sido confirmada en su vigencia por dos leyes posteriores: La Ley 9/2014, de 9 de mayo, General de las Telecomunicaciones, y la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que en sus respectivos artículos 42 y 52 remiten a la Ley 25/2007 en todo lo concerniente a la conservación y de cesión de datos con fines de detección, investigación y enjuiciamiento de delitos graves. Por lo tanto, el Legislador no sólo no ha dudado de la legalidad de la ley de referencia, sino que la ha confirmado expresamente en las dos leyes posteriores, precisamente las leyes que han establecido la regulación básica en este ámbito normativo.

La anulación de la Directiva 2006/24/CE nos podría llevar a considerar nula la ley española de desarrollo, pero semejante automatismo no es admisible. La Directiva en cuestión no fue anulada por un único motivo. El TJUE realizó un profundo análisis de conjunto y detectó deficiencias diversas o ausencia de controles también diversos que conferían a la norma comunitaria una laxitud que daba como resultado la ausencia de protección suficiente de los derechos fundamentales afectados. La interacción de esas deficiencias es lo que motivó la declaración de nulidad.

Así, se analizaron factores como los siguientes: a) Afección generalizada a todas las personas sin vinculación directa o indirecta a acciones

penales; b) Ausencia de límites temporales o geográficos que vinculen la conservación con hechos delictivos concretos o que permitan contribuir a la prevención, detección o enjuiciamiento de delitos graves; c) Falta de precisión respecto de las personas que puedan tener acceso y posterior uso de los datos; d) Ausencia de criterios objetivos respecto al uso posterior de los datos a lo estrictamente necesario, sin supeditarlo a un previo control judicial o de un organismo autónomo independiente; e) Ausencia de criterios objetivos para que la cesión se limite estrictamente a fines de prevención y detección de delitos graves; f) Establecimiento de un plazo de conservación único sin distinción entre la categoría de datos; g) Falta de un alto nivel de protección y seguridad de los datos conservados, a través de medidas técnicas y organizativas, frente a abusos y accesos ilícitos y que garanticen la integridad y confidencialidad de los datos.

Si hacemos ese análisis en la normativa española se puede comprobar que gran parte de las deficiencias advertidas en la Directiva anulada no se producen en nuestro ordenamiento jurídico. Destacamos, a este respecto, las siguientes notas:

> *(i) La ley española obliga a la conservación de datos de tráfico y localización durante un año y permite su cesión a las autoridades judiciales, si bien esa cesión está sujeta a estrictas garantías.*
>
> *(ii) Los prestadores de servicios obligados por ley a la conservación de datos no pueden realizar operación alguna de tratamiento, a salvo de la cesión singularizada que pueda recabar la autoridad judicial.*

Esto es importante, porque la doctrina del TJUE ha tenido como finalidad esencial la protección de los derechos a la vida privada, a la protección de datos y a la libertad de expresión, hasta el punto de en sus sentencias se ha insistido en que los datos conservados "considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan" (STJUE de la Gran Sala de 8 de abril de 2014 (TJCE 2014, 104) - Caso Digital Rights- 27).

La Ley española no genera ese riesgo. Los datos conservados permanecen custodiados y no pueden tener más uso que su cesión a la autoridad judicial cuando ésta, lo ordene bajo un riguroso sistema de garantías. Ciertamente la conservación de datos y la obligación de cesión es en sí "tratamiento de datos" y así lo ha reiterado el TJUE en varias de sus sentencias para afirmar la competencia del derecho comunitario sobre esta cuestión, pero no puede desconocerse que los obligados por la Ley 25/2007 sólo deben y pueden almacenar los datos, pero no están habilitados para realizar ninguna de las operaciones de tratamiento que podrían ser especialmente lesivas para los derechos que se pretenden salvaguardar. Los prestadores no pueden, por tanto, estructurar, seleccionar, divulgar, transmitir, combinar o utilizar para fines de investigación criminal esos datos.

(iii) Sólo cabe ceder los datos conservados para la detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en leyes especiales (artículo 1.1), precepto que antes debía ser integrado acudiendo a los artículos 13.1 y 33.1 CP y actualmente acudiendo al artículo 579.1 de la LECrim que sólo autoriza este tipo de injerencias en delitos castigados con al menos pena de prisión de 3 años, en delitos de terrorismo y en el delitos cometidos por grupos u organizaciones criminales.

(iv) Los datos que deben conservarse son los necesarios para rastrear e identificar el origen y destino de una comunicación, el tipo de comunicación y el equipo de comunicación de los usuarios (artículo 3.1) pero en ningún caso se pueden conservar datos que revelen el contenido de la comunicación (artículo 3.2)

(v) Los datos sólo pueden ser cedidos previa autorización judicial (artículo 6.1) y la resolución judicial que autorice la cesión deberá ser motivada y ajustarse a los principios de necesidad y proporcionalidad, especificando los datos que han de ser cedidos (artículo 7.2). Esta garantía es esencial y muchas de las legislaciones de los Estados de la Unión autorizaban la cesión a autoridades no judiciales.

(vi) La cesión se limita a su utilización en investigaciones penales por delitos graves (artículo 7) y no cabe la conservación o cesión para finalidades distintas de la investigación penal, como ha ocurrido en otras legislaciones, ni para la investigación de delitos de escasa entidad

(vii) Los datos sólo pueden ser cedidos a agentes especialmente facultados, señalando como tales a los miembros de los Cuerpos Fuerzas de Seguridad del Estado, Agentes de Vigilancia Aduanera y agentes del CNI) y deberán limitarse a la información imprescindible (artículo 6.2);

(viii) La ley impone a los sujetos obligados todo un conjunto de obligaciones para garantizar la integridad, seguridad, calidad y confidencialidad de los datos en el artículo 8 y establece un régimen de sanciones para caso de incumplimiento (artículo 11). Además, hay todo un desarrollo reglamentario que detalla las especificaciones técnicas en la forma de cesión de las operadoras a los agentes (Orden PRE/199/2013, de 29 de enero, que en todo caso ha de limitarse a lo estrictamente necesario. Y la ley española prevé un nivel de seguridad medio para este tipo de ficheros lo que garantiza la confidencialidad de los datos almacenados (artículo 81.4 del Real Decreto 1720/2007, de 21 de diciembre sobre Reglamento de Protección de Datos).

(ix) La Ley de Enjuiciamiento Criminal ha realizado una completa regulación de las intervenciones telefónicas y telemáticas, incluyendo en ellas el uso de los datos conservados por obligación legal (artículo 588 ter j), sujetando todas ellas a un estricto control judicial en su adopción y en su ejecución, con aplicación de los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad.

Conviene destacar que el uso de los datos almacenados está sujeto a estrictas limitaciones que se contienen en los artículos 588 bis a) y siguientes de la LECrim, entre las que destacamos:

(i) La utilización de datos está sujeta al principio de especialidad, de forma que sólo podrá autorizarse cuando la injerencia esté relacionada con un delito concreto.

(ii) No pueden autorizarse injerencias prospectivas, es decir, que tengan por objeto prevenir o descubrir delitos de forma indiscriminada o sin base objetiva.

(iii) La injerencia debe definir su ámbito objetivo y subjetivo conforme al principio de idoneidad.

(iv) La injerencia está también sujeta a los principios de excepcionalidad y necesidad sólo puede acordarse si no existen otras medidas menos gravosas y sólo cuando sea imprescindible

Por tanto, es cierto que muchos de los déficits de normatividad de la Directiva anulada por el TJUE no se dan en nuestra ordenación nacional al establecer garantías suficientes para que los datos personales conservados por obligación legal están suficientemente protegidos frente al riesgo de abuso ilegal tanto en relación con el acceso a esos datos como en el uso de los mismos. Y esa es la razón por la que esta Sala en anteriores sentencias ha considerado que nuestro ordenamiento en materia de conservación y cesión de datos es conforme con el derecho de la Unión. (…)

Teniendo en cuenta lo anterior, el juicio de proporcionalidad no solo se derivará de la propia la Ley 25/2007 de 18 de octubre, sino que ha de entenderse completado con las indicaciones que la LECrim prevé para el acceso a la información que se considera datos de tráfico -vinculadas a una comunicación concreta- y a aquellas necesarias para proceder a la posterior interceptación de las comunicaciones, y también para las que simplemente busquen la identificación de los usuarios al margen de un concreto proceso de comunicación.(Articulo 588 ter m LECrim)

Así se desprende del artículo 588 bis a que bajo la denominación “Principios rectores” inaugura el Capítulo IV referido a las “Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas”, al indicar que:

1.Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

(…)

5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad

de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Dicho lo anterior la Directiva 2002/58/CE de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, establece en su artículo 15.1 bajo la denominación "Aplicación de determinadas disposiciones de la Directiva 95/46/CE" lo siguiente:

> *1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.*

Pues bien, sobre la normativa de los Estados Miembro que habilite o permita el acceso a los datos personales generados en el ámbito de las comunicaciones electrónicas, la jurisprudencia europea ha sostenido la siguiente doctrina:

En primer lugar, cabe citar la STJUE de fecha 2/03/2021 en el Asunto C-746/18:

> *34 En particular, se ha declarado al respecto que las medidas legislativas relativas al tratamiento de datos referidos a la identidad civil de los usuarios de los medios de comunicaciones electrónicas como tales, en particular a su conservación y al acceso a los mismos, con el único objetivo de identificar al usuario de que se trate, y sin que dichos datos puedan vincularse a informaciones relativas a las comunicaciones efectuadas, pueden estar justificadas por el objetivo de prevenir,*

investigar, descubrir y perseguir ***delitos en general****, al que se refiere el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 . En efecto, dichos datos no permiten, por sí solos, conocer la fecha, la hora, la duración y los destinatarios de las comunicaciones efectuadas, ni los lugares en los que se produjeron estas comunicaciones o la frecuencia de las mismas con ciertas personas durante un período de tiempo determinado, por lo que no facilitan, al margen de las coordenadas de los usuarios de los medios de comunicaciones electrónicas, como sus direcciones, ninguna información sobre las comunicaciones transmitidas y, en consecuencia, sobre su vida privada. De este modo****, la injerencia que supone una medida relativa a estos datos no puede, en principio, calificarse de grave*** *(…)*

42. *Ante la inexistencia de normas de la Unión en la materia****, corresponde al ordenamiento jurídico interno de cada Estado miembro, en virtud del principio de autonomía procesal, configurar la regulación procesal de los recursos destinados a garantizar la salvaguardia de los derechos que el Derecho de la Unión confiere a los justiciables****, a condición, sin embargo, de que no sea menos favorable que la que rige situaciones similares de carácter interno (principio de equivalencia) y de que no haga imposible en la práctica o excesivamente difícil el ejercicio de los derechos conferidos por el Derecho de la Unión (principio de efectividad)-*

Por su parte la STJUE de fecha 6/10/2020 en los Asuntos C-511/18, C-512/18 y C-520/18 indica lo siguiente:

140.En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos, de conformidad con el ***principio de proporcionalidad****, solo la lucha contra la delincuentica grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, como las que supone la conservación de los datos de tráfico y de los datos de localización. En consecuencia****, solo las injerencias en tales derechos fundamentales que no presenten un carácter grave pueden estar justificadas por el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general****. (…)*

157.En lo tocante, por último, a los datos relativos a ***la identidad civil*** *de los usuarios de los medios de comunicaciones electrónicas, dichos datos no permiten, por sí solos, conocer la fecha, la hora, la duración y*

los destinatarios de las comunicaciones efectuadas, ni los lugares en los que se produjeron estas comunicaciones o la frecuencia de las mismas con ciertas personas durante un período de tiempo determinado, por lo que no facilitan, al margen de las coordenadas de estos, como sus direcciones, ninguna información sobre las comunicaciones transmitidas y, en consecuencia, sobre su vida privada. De este modo, ***la injerencia que supone la conservación de estos datos no puede, en principio, calificarse de grave****.*

158.De ello se sigue que, conforme a lo expuesto en el apartado 140 de la presente sentencia, las medidas legislativas relativas al tratamiento de estos datos como tales, en particular a su conservación y al acceso a los mismos con ***el único objetivo de identificar al usuario*** *de que se trate, y sin que dichos datos* ***puedan vincularse a informaciones relativas a las comunicaciones efectuadas****,* ***pueden estar justificadas*** *por el objetivo de prevenir, investigar, descubrir y perseguir* ***delitos en general****, al que se refiere el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 62).*

Finalmente, la STJUE de fecha 2/10/2018 en el Asunto C-207/16 indica lo siguiente*:*

"el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, ***constituye una injerencia*** *en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales,* ***que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave."***

De la lectura de las sentencias se deduce que la identificación de los usuarios de servicios de telecomunicaciones al margen de un proceso de comunicación concreto, **no se estima una injerencia grave en la privacidad y tampoco deben estar limitadas únicamente a la persecución de delitos graves y que por tanto las medidas legislativas que regulen dicho acceso se presumen acordes con el principio de proporcionalidad**.

Pues bien, a estos efectos debe tenerse en cuenta que en el artículo 588 ter m) de la LECrim bajo la denominación "Identificación de titulares o terminales o dispositivos de conectividad" se establece lo siguiente:

> *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.*

El precepto podrá tener cabida en aquellas solicitudes de información que **no esté vinculado necesariamente a un proceso de comunicación concreto**. Piénsese, por ejemplo, en un anuncio, en el que el medio de contacto es una línea de teléfono y se tienen indicios de que se promueve la venta de artículos procedentes de la comisión de delitos, o una oferta de trabajo en el que el nº de contacto es fundamental para perseguir un delito contra los derechos de los trabajadores. O como en el caso que se plantea, que se pretende conocer la titularidad del dispositivo físico -quien está detrás de un IMEI- en el que se ha introducido el duplicado de una tarjeta, a partir de un IMSI y se ha producido una conexión -que no comunicación- entre dicho dispositivo y la red.

En estos casos, la petición no estaría vinculada a un proceso de comunicación en concreto y por tanto tal como recuerda el apartado 34 de la STJUE de fecha 2/03/2021, el conocimiento de estos datos de identificación no permite por sí solo conocer aspectos de la vida privada de sus titulares.

Debe recordarse que el citado precepto se introduce por la modificación operada por la *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*, en cuya *Exposición de Motivos* se hace constar:

> *En la investigación de algunos hechos delictivos, la incorporación al proceso de los datos electrónicos de tráfico o asociados puede resultar de una importancia decisiva. La reforma acoge el criterio fijado por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, e impone la exigencia de autorización judicial para su cesión a los*

agentes facultados, ***siempre que se trate de datos vinculados a procesos de comunicación.*** *Su incorporación al proceso solo se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones. Se da un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia. También* ***se regula el supuesto de 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.*

Como puede observarse la reforma legislativa sigue el criterio fijado por la Ley 25/2007 de 18 de octubre, en cuanto a la exigencia de autorización judicial **para aquella información vinculada a un proceso de comunicación**.

Véanse los artículos 588 ter j a l de la LECrim, en la que se regula el acceso a determinada información con carácter previo a la solicitud de interceptación de la comunicación y para el acceso a los datos de tráfico.

Por lo que, de acuerdo con lo expuesto, la aplicación de la Ley 25/2007 y de los preceptos de la LECrim, coexisten y se complementan para garantizar la aplicación del principio de proporcionalidad.

A lo que hay que añadir que respecto de la necesidad de ley especial que pudiera derivarse de la STJUE que anula la Directiva 2006/24/CE, debe tenerse en cuenta que los preceptos de la LECrim que son de aplicación a estos supuestos han sido introducidos por una Ley Orgánica que aborda por razón de la materia y especialidad, aquellas concesiones en el derecho a la privacidad de los usuarios de servicios de telecomunicaciones. **Todo ello de conformidad con el apartado 42 de la STJUE de 2/03/2021 (y por tanto posterior a la STJUE que anula la Directiva) que hace una remisión a la normativa procesal de cada Estado de la Unión para regular dicha materia ante la ausencia de normativa europea al efecto.**

Asimismo, debe indicarse que la información referida al IMSI, al IMEI o la dirección IP cuyo acceso y tratamiento se regula los artículos precedentes de la LECrim (588 ter K e l) prevén el acceso a dicha información con la finalidad de proceder posteriormente a la interceptación de las comunicaciones, cuestión

que **no tiene por qué suceder en todos los supuestos,** como aquellos en los que se pretenda conocer la identificación de quién está detrás de un determinado IMSI o IMEI sin vinculación a un proceso de comunicación en concreto, sino a un proceso de conexión entre el dispositivo y la red de telefonía, para lo que se utilizaría la facultad que prevé el Artículo 588 ter m).

En este sentido procede citar lo indicado en la **Circular 2/2019 de 6 de marzo, sobre interceptación de comunicaciones telefónicas y telemáticas** de la Fiscalía General del Estado (Circular 2/2019 FGE) a cuyo tenor:

> *Es más, la gran mayoría de los casos en los que el Ministerio Fiscal o la Policía Judicial pudieran hacer uso de esta facultad podrían no tener relación, ni siquiera, con la preparación de una ulterior intervención de comunicaciones. En consecuencia, esta facultad no debe entenderse circunscrita a los supuestos de interceptación de comunicaciones que contempla el art. 588 ter a.*

De lo expuesto hasta ahora se ha de concluir que el acceso por parte de FCS y/o del Ministerio Fiscal a determinada información sobre comunicaciones electrónicas que obren en poder de las operadoras que prestan el servicio de telecomunicaciones, debe respetar en todo caso **el principio de proporcionalidad**, y que unas veces será el juez que debe autorizar una determinada medida quien le competa el juicio de proporcionalidad, y en las que no es necesaria dicha autorización, será al propio legislador al que se le presuponga dicha consideración.

Por eso no resulta invalidante, como se ha afirmado en el seno del GT1 creado al efecto, que en la Ley 25/2007 de 18 de octubre, no se regule expresamente el acceso a determinada información para la persecución, ex profeso, de las estafas SIM Swap, sino que **habrá de ser la interpretación de todas las circunstancias y la norma aplicable al caso concreto, las que nos proporcionen si la medida en concreto supera el test de proporcionalidad** al que aluden tanto la STJUE que anula la Directiva 2006/24/CE (STJUE de 8 de abril de 2014, Asunto C-293/2012) como las otras que se acaban de citar, y los preceptos de la propia LECrim de los que se desprende el cumplimiento del principio de proporcionalidad, y cuya legitimación también se deriva del apartado 42 de la STJUE 2/03/2021 que hace una remisión a la normativa procesal nacional ante la ausencia de norma comunitaria que sea de aplicación.

Sobre todo, si se tiene en cuenta que dichas peticiones de información pueden no estar vinculadas a un proceso de comunicación concreto lo que haría que no se aplicara la citada Ley 25/2007 de 18 de Octubre.

IV

Planteados los términos esenciales de la cuestión objeto de análisis es preciso abordar el régimen jurídico aplicable a los datos que se contienen en la información requerida por las FCS y el Ministerio Fiscal a las operadoras para investigar el SIM Swapping.

Como punto de partida deben abordarse los conceptos de "comunicación", "datos de tráfico" y "datos de abonado o de identificación", pues van a determinar la aplicación de distintos regímenes jurídicos.

En cuanto a la "comunicación", nos indica el artículo 2 de la Directiva 2002/58/CE, que considera como tal a *cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información*;

Ahora bien, en la citada comunicación existirán dos partes que serán de un lado el emisor y de otro el receptor, pero debe restringirse dicho concepto a procesos de comunicación entre seres humanos y no cuando uno de ellos es una máquina.

En efecto, no es lo mismo la transmisión de señales entre entes de carácter impersonal que la comunicación entre personas, (titulares de derechos subjetivos).

Como se ha dicho antes, una página web que aloja un anuncio fraudulento y se está investigando la dirección IP del servidor que aloja la página, o una página web con contenidos de protegidos por derechos de autor o con pornografía infantil y que se vigila al usuario que ha accedió al contenido.

En estos casos se investigará la comunicación entre su equipo o terminal y el servidor que aloja esas páginas webs y así la comunicación por parte de la entidad que tutela el dato no exigiría autorización judicial por no afectar a un proceso comunicativo.

Idéntica naturaleza se podrá atribuir a la conexión entre un dispositivo, por ejemplo, un teléfono móvil y la red de telefonía, que sucede cuando se enciende aquel, pues no estamos ante una comunicación en los términos indicados.

El artículo 18.3 de la CE protege el secreto de las comunicaciones, y aunque no forme parte del contenido, datos relativos al momento, duración o destino de la comunicación también se sitúan al abrigo de ese derecho fundamental. De ahí que la normativa aplicable requiere la autorización judicial para su obtención (artículo 7.2 de la Ley 25/2007 y determinados preceptos de la LECrim)

En efecto, cuando se establece una comunicación por medios telemáticos, además del contenido de la misma, también se generan los datos de origen, destino y ruta del mismo, así como otros necesarios para la prestación y facturación del servicio por operadora.

Estos serán los considerados como “dato de tráfico”. Así, el Convenio de Ciberdelincuencia del Consejo de Europa de Budapest, de 23 de noviembre de 2001, ratificado por España mediante Instrumento de 17 de septiembre de 2010 , los define en su artículo 1.d) a *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.*

Por su parte la Directiva 2002/58/CE, considera “Datos de tráfico” a *cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma*;

Es decir, la información sobre el origen y destino de la comunicación y que no constituya el contenido del mensaje, sino su trayectoria es la que se conocerá como datos de tráfico.

Y, en tercer lugar, en cuanto a los “datos de abonado o de identificación del usuario”, serán aquellos de los que dispone la operadora para posibilitar la prestación del servicio y en definitiva la ejecución del contrato entre esta y el destinatario del servicio.

Pues bien, esta información también “acompañará” a los datos de tráfico en cada comunicación, **pero también podrá obtenerse al margen de la existencia de la mera comunicación, pues en unos casos, la operadora ya dispone de ella, y en otros, por ejemplo, cuando un dispositivo se conecta a la red dónde las operadoras pueden captar información (IMSI e IMEI) de la que se puede obtener la identidad del abonado.**

El citado Convenio sobre Ciberdelincuencia en su artículo 18.3 considera como “datos de abonado” a:

(…) 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;

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".

Cómo se ha indicado antes, del precepto se deduce que los datos de abonado serán aquellos que la operadora, en tanto que es parte del contrato de servicios de telecomunicaciones, dispondrá para la correcta prestación del mismo. **Y entre los que deben incluirse también aquellos referidos a una concreta petición de duplicado de tarjeta SIM pues es un elemento necesario para la prestación de dicho servicio**.

Esta diferenciación ha sido abordada por la Circular 2/2019 de 6 de marzo de la FGE, donde se indica lo siguiente:

A la hora de determinar qué datos aparecen vinculados a procesos de comunicación y cuáles no, suele distinguirse entre datos de naturaleza dinámica y los de naturaleza estática. Los primeros son los que se generan durante un proceso de comunicación, mientras que los segundos aparecen almacenados en las bases de datos de los prestadores de servicios de comunicación para posibilitar esas comunicaciones, pero no se generan como consecuencia de una comunicación concreta. A esta misma conclusión conduce la definición que, sobre los datos de tráfico, ofrece el art. 1.d del Convenio sobre la Ciberdelincuencia, que señala que 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".

El debate en cuanto a la necesidad de autorización judicial, sin embargo, ya no está en la determinación de qué datos afectan al derecho fundamental al secreto de las comunicaciones. A la vista de la nueva regulación de la LECrim pueden ahora distinguirse dos categorías de datos: los vinculados a un proceso de comunicación, cuya incorporación al proceso se regirá por lo previsto en el art. 588 ter j (excepción hecha de la dirección IP en los casos que prevé el art. 588 ter k) y el resto de los datos de tráfico, no vinculados a procesos de comunicación, entre los que el legislador ha destacado, en los arts. 588 ter l y m, la numeración IMSI e IMEI y los datos de identificación del titular de números telefónicos o los números que corresponden a un titular.

En el mismo sentido, la Sentencia del Tribunal Supremo de 18 de marzo de 2010, núm. 247/2010, hace una distinción similar, en referencia a que **una cosa son los datos que afectan al secreto de las comunicaciones y otra aquellos que, sin estar referidos a un proceso de comunicación determinado se someten a tratamiento como datos estáticos por las operadoras**:

"*Distinguimos pues dos conceptos:*

a) Datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el art. 18-3 C.E EDL 1978/3879:

b) Datos o circunstancias personales referentes a la intimidad de una persona (art. 18-1º C.E. EDL 1978/3879), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o habeas data del art. 18-4 C.E. EDL 1978/3879 que no pueden comprometer un proceso de comunicación.

Desde esta perspectiva dicotómica la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un auténtico desenfoque del problema, pues incorporaría en el ámbito de la protección constitucional del art. 18-3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la autodeterminación informática del art. 18-4 C.E. EDL 1978/3879 (véase por todas S.T.S. núm. 249 de 20-5-2008 EDJ 2008/90719)".

Como puede observarse, el elemento diferenciador será si los datos están vinculados a un proceso de comunicación o si no lo están, y las consecuencias jurídicas serán que los primeros estarán bajo la protección del artículo 18.3 de la CE, la Ley 25/2007 y determinados preceptos de la LECrim, y los segundos serán aquellos objetos de protección por el artículo 18.4 de la CE y el régimen jurídico del derecho a la protección de datos personales.

V

Tradicionalmente la doctrina jurisprudencial sobre el IMSI y el IMEI se centró en si para su captación o conocimiento, era necesario autorización judicial y por tanto si se enmarcaban en el proceso de comunicación. Las Sentencias del Tribunal Supremo nº 249/08, de 20 de mayo, 460/2011 de 25 de mayo, vinieron a admitir que no era necesaria la autorización judicial para captar o conocer el IMSI o el IMEI y que su tratamiento por parte de las FCS era conforme al artículo 22 de la hoy derogada LOPD.

Ahora bien, también se sostenía que para solicitar a la operadora la identidad del titular del IMSI o del IMEI ya si era necesaria dicha autorización judicial por así indicarlo la propia Ley 25/2007, de 18 de octubre, que protege los “datos de tráfico”, es decir, vinculados a un proceso de comunicación concreto.

En este sentido el articulo 588 ter j de la LECrim bajo la denominación “Datos obrantes en archivos automatizados de los prestadores de servicios” indica que

> 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.

Como puede observarse resulta una condición necesaria para aplicar el precepto que los datos “se encuentren vinculados a un proceso de

comunicación". Lo que se interpreta que, sensu contrario, cuando no lo estén podrán obtenerse al amparo de otro presupuesto legal, como puede ser el previsto en el artículo 588 ter m) antes citado.

En efecto, en el presente caso podría resultar no exigible la solicitud de autorización judicial, pues las peticiones que las FCS y/o la Fiscalía soliciten a las operadoras sobre la "vinculación entre el IMSI y el IMEI" y que requieren un proceso de identificación, **no irían referidas a un concreto proceso de comunicación interpersonal**, sino a lo sumo, se deduciría de un proceso de conexión entre el dispositivo (al que le corresponde el IMEI y que alberga un IMSI) y la red de telefonía en cuestión).

Es decir, los datos solicitados serian aquellos derivados de la propia contratación y prestación del servicio y en particular por la "conexión" a la red del dispositivo en el que se utiliza una determinada tarjeta SIM (que es la que nos da el IMSI), es decir, **se generan ex ante y con independencia de la existencia de comunicación**.

En este sentido la citada Circular 2/2019, de 6 de marzo de la FGE, indica que:

> *En cuanto a los concretos datos que pueden ser recabados directamente por el Ministerio Fiscal o por la Policía Judicial, la previsión no se agota, simplemente, en la obtención de la titularidad de un número de teléfono o, en sentido inverso, en la obtención del concreto número telefónico que utilice una persona, sino que debe entenderse aquí incluida cualquier petición de datos encaminada a esa identificación del titular o del dispositivo de comunicación,* ***siempre que no se trate de datos vinculados a procesos de comunicación.***
>
> *Se incluirían aquí, por ejemplo, los supuestos de solicitud del IMSI que aparece asociado a un determinado dispositivo electrónico,* ***con el fin de determinar quién es el usuario de ese dispositivo electrónico****. Este supuesto se ha venido planteando con cierta frecuencia en los casos de sustracción de teléfonos móviles con el fin de identificar a la persona que lo tenía en su poder mediante la identificación del IMSI de la tarjeta SIM que estaba siendo utilizada por el usuario del teléfono. El* ***IMSI, en estos casos, no puede ser considerado como un dato de tráfico y, por lo tanto, vinculado a un proceso de comunicación****, pues no se genera como consecuencia de una comunicación concreta, sino que se trata, en palabras de la STS nº 249/2008, de 20 de mayo, de un código de identificación de cada dispositivo de telefonía móvil que sirve para posibilitar esa identificación a través de las redes GSM y*

*UMTS; en consecuencia, puede fácilmente encuadrarse en el concepto de "**dato identificativo de un medio de comunicación**", que utiliza el art. 588 ter m. Se trata, por lo tanto, de un supuesto diferente al que regula el art. 588 ter l en el que, como antes se analizaba, será necesario recabar autorización judicial para relacionar ese IMSI con otros datos que posibiliten la identificación del usuario.*

Sobre el tratamiento del IMSI y del IMEI en relación con la aplicación del artículo 588 ter m) LECrim los tribunales ordinarios de justicia se han pronunciado, sirva la Sentencia de la Audiencia Provincial de Barcelona núm. 390/2019 de 30 de mayo, que dispone:

"*Sin embargo, la identidad del titular de la tarjeta SIM, o lo que es lo mismo, la identidad del titular del número de teléfono asociado a dicha tarjeta no constituye un dato de tráfico derivado de las comunicaciones telefónicas ni un dato que afecte a la comunicación misma.*

No cabe duda de que constituye un dato personal relativo a la intimidad de la persona amparada en el art. 18.1 CE.

Pero como ha tenido ocasión de expresar el Tribunal Constitucional no toda injerencia en el derecho fundamental a la intimidad está alcanzado por la reserva absoluta de previa resolución judicial, como sucede en el ámbito de las comunicaciones telefónicas, electrónicas o telegráficas (art. 18.3 CE); y aunque en ocasiones se ha reclamado por parte del Alto Tribunal la exigencia de resolución judicial previa, "no es menos cierto que sólo hemos exigido dicha decisión "como regla general" (STC 71/2002, de 3 de abril , FJ 10 a)]. En efecto, hemos señalado que, "a diferencia de lo que ocurre con otras medidas restrictivas de derechos fundamentales que pueden ser adoptadas en el curso del proceso penal (como la entrada y registro en domicilio del art. 18.2 CE o la intervención de comunicaciones del art. 18.3 CE), respecto de las restricciones del derecho a la intimidad (art. 18.1 CE) no existe en la Constitución reserva absoluta de previa resolución judicial" (SSTC 234/1997, de 18 de diciembre (RTC 1997, 234) , FJ 9, in fine ; 70/2002, de 3 de abril , FJ 10.b.3; en el mismo sentido, STC 207/1996, de 16 de diciembre FJ 4 c)]. De manera que, en la medida en que no se establece en el art. 18.1 CE reserva alguna de resolución judicial, como hemos señalado en otras ocasiones, "no es constitucionalmente exigible que sea el Juez quien tenga que autorizar esta medida limitativa, pudiéndola adoptar, siempre que una ley expresamente la habilite, la autoridad que, por razón de la

materia de que se trate, sea la competente" (STC 234/1997, de 18 de diciembre, FJ 9, in fine)".

El legislador, siguiendo la anterior doctrina, ***ha regulado por ley el modo de obtención de la información correspondiente a la identidad del titular de un determinado teléfono****, previniendo que en los casos en que, 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 (art. 588 ter m LECrim*)"

En el mismo sentido la Sentencia de la Audiencia Provincial de Ciudad Real núm. 191/2019 de 31 octubre, establece lo siguiente en relación con la consideración del IMEI y la finalidad concreta de conocer quién activó una tarjeta SIM (…) *Sin embargo, la identidad del titular de la tarjeta SIM, o lo que es lo mismo, la identidad del titular del número de teléfono asociado al IMEI, no constituye un dato de tráfico derivado de las comunicaciones telefónicas ni un dato que afecte a la comunicación misma.(…) a los efectos que aquí interesa sólo era necesario determinar quien en su día activó el terminal, lo que era suficiente*(…).

Sobre la entrega de los datos identificativos del IMEI o del IMSI el citado ANEXO I del Dictamen 1/19 indica que

> 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.

Finalmente, también debe indicarse que en la Disposición adicional única de la Ley 25/2007 de 18 de octubre, referida a "*Servicios de telefonía mediante tarjetas de prepago*", en síntesis, se establece la creación de un

registro (libro-registro) con información identificativa sobre los titulares de tarjetas prepago y la obligación de su comunicación a los agentes facultados cuando les sean requeridos, sin que se haga mención alguna sobre la necesidad de obtención de mandamiento judicial:

> *1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.*
>
> *Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.*
>
> *La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.*
>
> *2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.*
>
> *3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.*

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

Pues bien, debe tenerse en cuenta que, en definitiva, el citado libro registro contiene información identificativa sobre el titular de los servicios contratados o adquiridos mediante la tarjeta de prepago, así como la documentación sobre la acreditación de la personalidad.

Proceso que no dista mucho de aquel que se produce cuando se tramita una solicitud de duplicado de una tarjeta SIM, en cuyo caso se requerirá al menos la validación de una identidad previo cotejo con algún documento acreditativo de la identidad, para así vincular un IMSI, o mejor dicho una línea de teléfono a una persona en concreto.

Por lo tanto, la interpretación del sentido de esta disposición adicional en referencia al caso objeto de consulta, *mutatis mutandi,* debe ser que si para acceder a los datos del libro-registro de tarjetas de prepago (que a fin de cuentas contienen datos identificativos) no se exija autorización judicial, resulta ilógico que las operadoras muestren dudas sobre su necesidad, cuando se les requiera información (muy similar teniendo en cuenta la finalidad del libro-registro), referida a un proceso de duplicación de una tarjeta SIM entre lo que debe incluirse la documentación que se utilizado, y la vinculación entre el IMSI y el IMEI. En ambas situaciones, el denominador común será la ausencia de proceso de comunicación y la finalidad de identificar a la persona a la que se asocia el servicio y el dispositivo.

En definitiva, cabe concluir que el IMSI y el IMEI, no pueden revestir, siempre y en todo caso, las garantías que prevé la Ley 25/2007 de 18 de octubre, y en último término las referidas al derecho fundamental al secreto de las comunicaciones, en cuyo caso su acceso siempre requeriría de autorización judicial. Sino que como indica el articulo 588 ter m) de la LECrim será posible su acceso a los fines indicados en dicho precepto, siempre y cuando la petición no se encuentra vinculada a un proceso de comunicación concreto.

VI

En cuanto a la consideración que deben tener el IMSI y el IMEI desde la perspectiva del derecho a la protección de datos, debe indicarse que esta Agencia ha tenido ocasión de pronunciarse en distintos informes que conviene trae a colación.

En el Informe 134/2019 se indicaba lo siguiente:

(…) Reiterando que el tema ha sido tratado por el Grupo de Trabajo de Autoridades de Protección de Datos, creado por el artículo 29 de la Directiva 95/46/CE, ha de partirse del Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio (documento WP 136), que recuerda que es posible hablar de la existencia de datos personales incluso en supuestos en los que ***no se cuenta con una identificación singularizada*** *del interesado, dado que:*

"(...) conviene señalar que, si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. También en Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos. La definición de datos personales refleja este hecho. (...) Las autoridades nacionales de protección de datos se han enfrentado a casos en los que el responsable del tratamiento sostenía que sólo se habían tratado informaciones dispersas, sin referencias a nombres u otros identificadores directos, y abogaba por que los datos no se considerasen como personales y no estuvieran sujetos a las normas de protección de los datos. Y, sin embargo, el tratamiento de esa información sólo

cobraba sentido si permitía la identificación de individuos concretos y su tratamiento de una manera determinada. En estos casos, en los que la finalidad del tratamiento implica la identificación de personas, puede asumirse que el responsable del tratamiento o cualquier otra persona implicada tiene o puede tener medios que «puedan ser razonablemente utilizados», para identificar al interesado. De hecho, sostener que las personas físicas no son identificables, cuando la finalidad del tratamiento es precisamente identificarlos, sería una contradicción flagrante. Por lo tanto, debe considerarse que la información se refiere a personas físicas identificables y el tratamiento debe estar sujeto a las normas de protección de datos."

Y en cuanto a la posibilidad de identificación del interesado, el documento además recuerda lo siguiente: "Por otra parte, se trata de una prueba dinámica, por lo que debe tenerse en cuenta el grado de avance tecnológico en el momento del tratamiento y su posible desarrollo en el período durante el cual se tratarán los datos. Puede que la identificación no sea factible hoy con el conjunto de los medios que puedan ser razonablemente utilizados en la actualidad. Si lo previsto es que los datos se conserven durante un mes, puede que no sea factible adelantar la identificación para que esté terminada dentro del «período de vida» de la información y, por lo tanto, esa información no debe considerarse como datos personales. Ahora bien, si el período de conservación previsto es de diez años, el responsable del tratamiento debe barajar la posibilidad de que la identificación pueda producirse al cabo de nueve años, con lo que adquiriría en ese momento la categoría de datos personales. Es preciso que el sistema sea capaz de adaptarse a los progresos tecnológicos a medida que éstos se produzcan y que introduzca las medidas técnicas y organizativas apropiadas a su debido tiempo."

Y más específicamente en relación con el asunto que nos ocupa, esta opinión se singulariza ***en relación con los dispositivos de telefonía móvil que permiten la localización*** *del interesado en su Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes (documento WP185).*

En dicho documento, tras recordar las conclusiones ya alcanzadas en su anterior Dictamen 5/2005 (WP115), de las que se desprende que "debido a que los datos de localización que se obtienen de las estaciones base se refieren a una persona física identificada o

identificable, estos están sujetos a las disposiciones relativas a la protección de los datos de carácter personal que se establecen en la Directiva 95/46/CE del 24 de octubre de 1995", concluye, en lo que afecta a la aplicación de la citada Directiva, lo siguiente:

"Conforme a la Directiva sobre protección de datos, se entiende por datos personales toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social - artículo 2 (a) de la Directiva.

El considerando 26 de la Directiva presta especial atención al término "identificable" cuando señala: "considerando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona."

El considerando 27 de la Directiva expone el amplio alcance de la protección: "considerando que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión;"

En su Dictamen 4/2007 sobre el concepto de datos personales, el Grupo de Trabajo ha facilitado una amplia orientación sobre la definición de datos personales.

Dispositivos móviles inteligentes

Los dispositivos móviles inteligentes están inextricablemente ligados a las personas físicas. Normalmente existe una identificabilidad directa e indirecta.

En primer lugar, los operadores de telecomunicaciones que proporcionan acceso a Internet móvil y a través de la red GSM poseen normalmente un registro con el nombre, la dirección y los datos bancarios de cada cliente, junto con varios números únicos del dispositivo, ***como el IMEI y el IMSI****.*

En segundo lugar, la compra de software adicional para el dispositivo (de aplicaciones o apps) suele requerir un número de tarjeta de crédito y

de ahí que enriquezca la combinación del o de los números únicos y los datos de localización con datos directamente identificativos.

La identificabilidad indirecta puede lograrse mediante la combinación del o de los números únicos del dispositivo, junto con una o más ubicaciones calculadas.

Cada dispositivo móvil inteligente posee al menos un identificador único, la dirección MAC. El dispositivo puede tener otros números de identificación únicos, que puede añadir el desarrollador del sistema operativo. Estos identificadores pueden transmitirse y tratarse posteriormente en el contexto de los servicios de geolocalización. Es cierto que la ubicación de un dispositivo concreto puede calcularse de forma muy precisa, especialmente cuando se combinan las distintas infraestructuras de geolocalización. Dicha ubicación puede apuntar a una casa o a un empleador. Es posible, especialmente a través de las observaciones repetidas, identificar al propietario del dispositivo.

A la hora de considerar los medios disponibles para la identificabilidad, los avances deben tenerse en cuenta ya que las personas tienden a divulgar cada vez más datos de localización personal en Internet, por ejemplo, publicando la ubicación de su casa o su trabajo junto con otros datos identificables. Este tipo de divulgaciones también puede darse sin su conocimiento, cuando otras personas les geo etiquetan. Gracias a este avance resulta más fácil vincular una ubicación o un patrón de comportamiento con una persona específica.

Además, conforme al Dictamen 4/2007 sobre el concepto de datos de carácter personal, debe señalarse que un identificador único, en el contexto descrito anteriormente, permite realizar un seguimiento de un usuario de un dispositivo específico y, por tanto, permite "singularizar" al usuario incluso aunque se desconozca su verdadero nombre."

(…)

II

En el mismo sentido que el Grupo de Trabajo del Art. 29 de la Directiva 1995/46/CE, esta Agencia ya trató la cuestión en los dos informes de 3 de junio de 2011, a los que se ha hecho mención anterior, estudiando un sistema también basado en la geolocalización de clientes, y señaló que:

> *"De todo lo anteriormente indicado parece desprenderse que el tratamiento conjunto de los datos relacionados con un terminal*

móvil, consistentes en el TMSI (que podría asimilarse con la dirección IP dinámica), ***la dirección MAC y el código IMSI (que podría equipararse a una suerte de dirección MAC de la tarjeta SIM del usuario****), implican la recopilación de información suficiente para que pueda entenderse que dicho tratamiento se encuentra sometido a lo dispuesto en la Directiva 95/46/CE y, por ende, en la Ley Orgánica 15/1999.*

(…)

En resumen, de lo señalado en la consulta no se deriva que la consultante, en mayor medida cuanto mayor sea su ámbito de actuación, podrá conocer los tres datos identificativos del terminal y de la tarjeta SIM del usuario, así como sus hábito de consumo, de forma que si resultase posible la asociación del titular con información adicional que permitiese una mayor identificación, el tratamiento podría perjudicar las garantías de su derechos fundamental a la protección de datos de carácter personal.

De este modo, sólo sería posible evitar la aplicación de la legislación de protección de datos en caso de que se produjese una disociación absoluta de los datos de TMS, IMSI y dirección MAC del terminal del usuario *y que dicha información no pudiera en ningún caso ser objeto de conservación por parte de la consultante; es decir, que se produjese un procedimiento de anonimización tal que resultase irreversible a la consultante conocer qué datos se ocultan bajo el número aleatorio asignado.*

En consecuencia, la atribución de tal número debería derivarse de la aplicación de un algoritmo que combinase los tres datos señalados y cuya aplicación resultase completamente irreversible, no conservándose por la consultante dato alguno de los enumerados en la consulta, aplicándose el algoritmo de forma inmediata en el momento de la recepción de la señal emitida por el terminal móvil.

Ciertamente en ese caso la consultante podría seguir teniendo información referente a hábitos de conducta del portador del terminal móvil, pero la misma no iría referenciada a datos que pudiesen permitir la identificación de tal usuario, sino a un dato derivado de la aplicación de un algoritmo irreversible, lo que

permitiría considerar que en el supuesto planteado se habría aplicado efectivamente un procedimiento de disociación en los términos establecidos en el artículo 3 f) de la Ley Orgánica 15/1999, que define como tal "Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Dicho lo anterior, deberían igualmente preverse normas de seguridad que impidiesen el acceso a la información por personal ajeno a la consultante, lo que parece derivarse de lo indicado en la consulta y el acceso a la información únicamente de forma agregada, tal como se señala en la misma.

(…).

Dicha conclusión resulta claramente extrapolable al escenario normativo actual, al amparo de las definiciones anteriormente transcritas, contenidas en el Reglamento General de Protección de Datos -RGPD- y en la Ley Orgánica 3/2018, de 5 de diciembre -LOPDGDD-.

Por su parte la STJUE de 19 de octubre de 2016 Asunto C-582/14, considera que incluso la dirección IP dinámica ha de considerarse dato de carácter personal en la medida en que el proveedor de servicios tiene medios puede conocer la identidad del titular de esa dirección IP de carácter dinámico.

O la más reciente STJUE de 17 de junio de 2021 Asunto C-579/19 que en su apartado 102 recuerda que (…)*Un dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal en el sentido del artículo 4, punto 1, del Reglamento 2016/679, cuando este disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional con que cuenta el proveedor de acceso a Internet de esa persona(…)*

Quiere decir esto que mientras exista la posibilidad de realizar la identificación estaremos ante un dato de carácter personal.

Es importante esta consideración en relación con el caso concreto, pues recuérdese que la dirección IP dinámica es aquella que cambia cada cierto tiempo, por ejemplo, por cambios en la red, o por la reiniciación del dispositivo con el que el proveedor de servicios proporciona la conexión, en contraposición a la dirección IP estática que siempre es la misma.

Si el TJUE considera dato personal dicha dirección IP dinámica, “que cambia cada cierto tiempo” es lógico considerar que el IMSI y el IMEI, que tienen un carácter permanente y del que se deriva, por tanto, una mejor individualización del usuario y también su identificación, puedan también tener dicha consideración.

Por lo tanto, de la lectura del informe parcialmente transcrito y de la STJUE indicada se deduce que tanto el IMEI, como el IMSI en la medida que permiten singularizar a un individuo, y por tanto identificarle, han de ser considerados datos de carácter personal de acuerdo con el artículo 4.1 del RGPD que considera como tal:

> *Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*

VII

A continuación, procede abordar el tratamiento de datos personales derivado de la comunicación del IMSI o del IMEI a las FCS y al Ministerio fiscal en la investigación y persecución de delitos.

En el Informe nº 213/2004 (y en idénticos términos el Informe nº 441/2003, Informe 297/2005 y en relación con la cesión de datos, en general, a las FCS el Informe nº 133/2008) emitido a la luz de la LOPD y el también derogado, artículo 12 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se abordaba una cuestión similar en los siguientes términos:

> *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.

Sobre la comunicación de datos personales para fines policiales la Sentencia del Tribunal Constitucional 14/2003 de 28 de enero, resalta la necesidad de justificación razonada en la recogida de tratamiento de dichos datos (FJ 7).

Asimismo, la Sentencia del Tribunal Supremo núm. 249/2008 de 20 de mayo, recuerda la relación entre el artículo 22 de la LOPD con el tratamiento de datos especialmente protegidos:

Esa capacidad de recogida de datos que la LO 15/1999, de 13 de diciembre, otorga a las Fuerzas y Cuerpos de Seguridad del Estado, no puede, desde luego, servir de excusa para la creación de un régimen incontrolado de excepcionalidad a su favor. Pero tampoco cabe desconocer que la recogida de ese dato en el marco de una investigación criminal -nunca con carácter puramente exploratorio-, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional. También parece evidente que esa legitimidad que la Ley confiere a las Fuerzas y Cuerpos de Seguridad del Estado nunca debería operar en relación con datos referidos al contenido del derecho al secreto de las comunicaciones (art. 18.3 de la C.E) o respecto de

datos susceptibles de protección por la vía del art. 18.4 de la C.E . que afectarán a lo que ha venido en llamarse el núcleo duro de la privacidad o, con la terminología legal, los datos especialmente protegidos (art. 7.2 LO 15/1999).

Es decir, se deduce la aplicación del artículo 22 de la LOPD con carácter general para la investigación de delitos, salvo para datos referidos al contenido al derecho al secreto de las comunicaciones, o al derecho a la protección de datos cuando estemos ante categorías especiales de datos en la denominación actual del artículo 9 del RGPD.

Por su parte, los tribunales ordinarios también han tenido ocasión de pronunciarse, por todas la Sentencia núm. 261/2018 de 23 de Octubre de la Audiencia Provincial de Cádiz en la que se ampara en el artículo 22 de la LOPD la cesión de los datos bancarios a la policía sin autorización judicial ni consentimiento del afectado.

En definitiva, el responsable o encargado no podría negarse a colaborar con la policía en el sentido de proporcionar datos personales que tuviera derivado de tal condición, *al amparo de la protección de los datos de sus clientes*, siempre y cuando existiera una petición concreta, debidamente motivada, y que no implicara un acceso masivo a datos personales y que fuera necesaria para la investigación, todo ello de acuerdo con el artículo 22 de la LOPD.

VIII

En la actualidad el RGPD determina en su artículo 2 bajo la denominación “Ámbito de aplicación material” lo siguiente:

2. *El presente Reglamento no se aplica al tratamiento de datos personales:*(…)

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Por su parte la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (LOPDGDD) establece en su artículo 2 bajo la denominación “Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94” lo siguiente:

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

(…)

Y en la Disposición transitoria cuarta Tratamientos sometidos a la Directiva (UE) 2016/680, lo siguiente:

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

En el BOE de 27 de mayo de 2021 se publicó la *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*, como norma de transposición de dicha Directiva, cuyo objeto y ámbito de aplicación se determina en sus artículos 1 y 2.1:

Artículo 1. Objeto.

Esta Ley Orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 2. Ámbito de aplicación.

1. Será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación

y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Teniendo en cuenta lo anterior, el tratamiento que está siendo objeto de análisis en el presente informe consistente en la comunicación de determinada informacion a las FCS y al Ministerio Fiscal, se sitúa bajo la aplicación del RGPD, sin perjuicio de que una vez que éstos tengan la información y por tanto sometan a tratamiento los datos personales, se sitúen al abrigo de la disposición de la citada Ley Orgánica 7/2021.

En este sentido, en el Informe nº 17/2021 sobre el Anteproyecto de la Ley de Enjuiciamiento Criminal, se analiza la coexistencia y aplicación de la citada Directiva y del presente RGPD, al indicar que:

> *En este sentido, es preciso recordar que la mencionada Directiva forma parte de la reforma operada en el régimen de protección de datos en el ámbito de la Unión Europea, complementando así, para los tratamientos incardinados en su ámbito de aplicación, el régimen general establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).*
>
> *A tal efecto, es relevante poner de manifiesto que la Directiva viene a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el Reglamento general de protección de datos. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento.*
>
> *(…)*
>
> *En relación con su ámbito de aplicación, debe nuevamente traerse a colación la ya referida mención al principio de especialidad, de tal modo que se encontrarán sometidos a lo dispuesto en el Anteproyecto aquellos tratamientos que, encontrándose dentro del ámbito de aplicación del derecho de la Unión, no están sometidos al régimen general establecido en el reglamento, debiendo además afectar el*

ámbito de aplicación a todos los tratamientos a los que se refiere la Directiva, sin que pueda excluirse de la protección del derecho fundamental ningún tratamiento incluido en dicho ámbito.

Por lo tanto, la comunicación de los datos personales referidos al IMSI, al IMEI, o a cualquier otra información referida a la vinculación entre ambos y a aquella derivada del proceso de duplicación de la tarjeta SIM, por parte de las operadoras a las FCS y/o al Ministerio Fiscal, está amparada en el artículo 6.1 c) del RGPD, a cuyo tenor:

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

(…)

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

Por su parte la LOPDGDD en su artículo 8 bajo la denominación "Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos" establece en su apartado 1 lo siguiente:

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

En este sentido la norma con rango legal que puede invocarse y que establece la obligación especifica es la LECrim, y en concreto los preceptos analizados, sin perjuicio de otras disposiciones del ordenamiento jurídico que imponen el deber de colaboración con las FCS y en su caso, con el Ministerio Fiscal.

Una vez cursada la petición y recibida la informacion por parte de las FCS y/o el Ministerio Fiscal, **el tratamiento de datos que realicen debe entenderse referido al realizado por las autoridades competentes** para *fines de prevención, investigación, detección o enjuiciamiento de infracciones*

penales, por lo que resulta de aplicación la citada *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*, tal como se indica en sus artículos 1 y 2.1 antes citados y de acuerdo con su ámbito subjetivo de aplicación, que en el artículo 4.1 a) y apartado 2 establece, qué se considera cómo autoridad competente:

> Artículo 4. Autoridades competentes.
>
> *1. Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.*
>
> *En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:*
>
> a) *Las Fuerzas y Cuerpos de Seguridad.*
>
> (…)
>
> *2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.*

Por su parte en el artículo 6 recoge los "*Principios relativos al tratamiento de datos personales",* indicando que los datos personales serán:

> *a) Tratados de manera lícita y leal.*
>
> *b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.*
>
> *c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.*
>
> *d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados.*
>
> *e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados.*

f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas.

Estos principios pueden considerarse la *actualización* y concreción de lo que se indicaba en los anteriores informes de esta Agencia y las sentencias citadas sobre los requisitos que debía cumplir el tratamiento de datos al amparo del derogado artículo 22 de la LOPD una vez que las autoridades competentes recibieran la información.

En cuanto a la licitud del tratamiento, establece el Artículo 11 lo siguiente:

1. El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones.

2. Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

En el presente caso, debe considerarse que la ley habilitante para el tratamiento de los datos referidos a los términos de la consulta ser la LECrim, y en su caso, la Ley 25/2007 de 18 de octubre.

Por otro parte, desde el lado de las operadoras y sin perjuicio de lo indicado en el artículo 6.1 c) del RGPD, debe recordarse lo indicado en el Artículo 7, que bajo la denominación “Deber de Colaboración” indica que:

1. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.

La comunicación de datos, informes, antecedentes y justificantes por la Administración Tributaria, la Administración de la Seguridad Social y la Inspección de Trabajo y Seguridad Social se efectuará de acuerdo con su legislación respectiva.

2. En los restantes casos, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

3. No será de aplicación lo dispuesto en los apartados anteriores cuando legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.

4. En los supuestos contemplados en los apartados anteriores, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Por lo tanto, las operadoras de telecomunicaciones están obligadas a proporcionar la información sobre la vinculación entre el IMEI y el IMSI, -**siempre que no se encuentre vinculado a un proceso de comunicación, en cuyo caso se necesitara autorización judicial**- así como los datos conexos al proceso de duplicación de la tarjeta SIM, no solo por lo indicado en el artículo 588 ter m) de la LECrim, sino también al amparo del deber de colaboración que se acaba de indicar, y sin perjuicio de que la comunicación de los datos se realizaría al amparo del artículo 6.1 c) del RGPD.

Por otra parte, debe recordarse que los responsables del tratamiento -las autoridades competentes- están sometidos a las obligaciones referidas a los plazos de conservación y revisión (artículo 8) y, entre otras, a las relativas a la “protección de datos desde el diseño y por defecto” previstas en el artículo 28 y la “seguridad del tratamiento” referida en el artículo 37 de la citada ley orgánica.

Por lo tanto, y en relación con el tratamiento objeto de análisis en la presente consulta, debe indicarse que del lado de las operadoras encuentra su legitimación en el artículo 6.1 c) del RGPD, y una vez que las FCS y/o el Ministerio Fiscal dispongan de los datos, dicho tratamiento se somete a la Ley Orgánica 7/2021, de 26 de mayo y por tanto, deberán cumplirse los principios referidos en el artículo 6, y en especial los de limitación de la finalidad y minimización (apartados b) y c)).

IX

Lo analizado hasta ahora es el tratamiento de los datos personales que obran en poder de las operadoras para facilitarlos a las FCS y/o al Ministerio Fiscal para la persecución del delito que hay detrás del SIM Swapping, sin embargo, es preciso indicar que este es un elemento o estadio del tratamiento de datos derivado de esta estafa, que tiene necesariamente unos antecedentes que es preciso analizar.

Del lado de las operadoras, debe indicarse que, con carácter general tratan los datos de sus clientes al amparo de lo previsto en el artículo 6.1 b) del RGPD, por considerarse un tratamiento necesario *para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.*

Y que, para completar la estafa, es necesario que el tercero “suplante la identidad” del titular de los datos, para recibir el duplicado de la tarjeta SIM.

Lo que conlleva a priori, un tratamiento al margen del principio de licitud pues un tercero está tratando datos, ya que tiene acceso a ellos, sin base legal alguna, además de la vulneración de otros principios como el de confidencialidad e integridad, que según indica el articulo 5.1 f) del RGPD, los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

Por dicha razón, este es un proceso en dónde la diligencia prestada por las operadoras es fundamental para evitar este tipo de estafas y vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que el tratamiento de datos es conforme al RGPD.

Por lo que, en tanto que responsables del tratamiento, les competen a las operadoras el cumplimiento de los principios recogidos en el artículo 5 del RGPD, entre los que cabe destacar el de lealtad, integridad y confidencialidad (apartados 5.1 a) y f)).

Asimismo, debe tenerse en cuenta lo indicado en el artículo 24 del RGPD a cuyo tenor:

> *1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

En segundo lugar, lo indicado en el artículo 25 del RGPD referido a la protección de datos desde el diseño y por defecto.

Y En tercer lugar el articulo 32.1 b) y d) del RGPD a cuyo tenor

> *Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> > *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> *(…)*
>
> > *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

Es decir, las operadoras deben de estar en disposición de establecer mecanismos que impidan que se produzcan la duplicación fraudulenta de las tarjetas SIM, medidas que respecten la integridad y confidencialidad de los datos y que impidan que un tercero acceda a datos que no son de su titularidad, pues precisamente compete a la operadora tratar datos de carácter personal conforme al RGPD.

A lo que hay que añadir la obligación que se deriva del principio de responsabilidad proactiva previsto en el artículo 5.2 del RGPD, es decir, no basta con no incumplir, sino que hay que demostrar que los tratamientos de datos se realizan conforme a la normativa vigente.

No puede repercutirse en el usuario las carencias de un sistema de emisión de duplicados que abarque los supuestos al margen del procedimiento físico, pues si la compañía ha establecido, entre otras, dicha posibilidad, debe en igual medida comprobar que el tratamiento de datos que sea necesario para tal fin (emisión del duplicado de la SIM) reviste de todas las garantías para cumplir con el RGPD.

En este sentido procede citar la Resolución R/01359/2008, puesto que se analiza el tratamiento de datos derivado de un proceso de contratación “a distancia” y dónde se pone de manifiesto la necesidad de que el responsable del tratamiento adecue las medidas para que dicho tratamiento sea conforme a derecho, (en aquel caso era necesario medidas que comprobaran la edad del contratante) sin que se pueda aducir que los riesgos asumidos son “propios del medio utilizado”, en concreto se señala:

> *Nadie puede alegar su propia falta de diligencia (en este caso, el procedimiento de comprobación de edad no funcionó, ni repercutir en el potencial cliente los errores derivados de las técnicas o mecanismos empelados para la contratación, como se deriva del propio artículo 10 LGCU.*
>
> *En la circunstancia del desconocimiento real de la edad de la menor, no puede ampararse TME. No es la menor la que toma la iniciativa en la relación contractual, habida cuenta de que se trata de un medio de contratación elegido por TME y que a sólo beneficia a ésta, de modo que no puede beneficiarse de un medio de comunicación que le imposibilita conocer el grado de capacidad de la contraparte. Es TME quien tiene que asumir los inconvenientes derivados de la falta de contacto física entre las partes contratantes.*

Inconvenientes que sólo TME está en disposición de evitar en estos casos, renunciando a captar el cambio de contratación vía telefónica y, siempre, solicitando la identificación de sus titulares, o realizando las comprobaciones necesarias, eficaces y efectivas para conocer la edad del menor, tanto por la adecuación a su actuar a la LOPD, como para asegurarse que la contratación se hace con todas las garantías y requisitos, que en Derecho, son recogidos en la Teoría General de Obligaciones y Contratos.

Son las operadoras las que tienen que asumir los riesgos derivados de la posibilidad de realizar duplicados sin presencia física, y estar en condiciones de eliminar dichos riesgos. En este sentido el artículo 28.2 LOPDGDD establece lo siguiente:

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

(…)

En conclusión, las operadoras de telecomunicaciones deben cumplir y estar en condiciones de demostrar que cumplen con el RGPD a la hora de llevar a cabo el tratamiento de datos personales derivado de la tramitación de la solicitud de duplicado de la tarjeta SIM, pudiendo incurrir en caso de no hacerlo en las conductas previstas en el régimen sancionador establecido en Título IX de la LOPDGDD.

X

Idénticas consideraciones merece la actuación de las entidades bancarias que proporcionan servicios de pago, en cuyo ámbito se inicia este tipo de estafas, ya que el tercero tiene acceso a las credenciales del usuario afectado y se hace pasar por este.

Es decir, la vulneración de la normativa de protección de datos y la de protección de pagos es el requisito que inicia la estafa SIM Swapping.

En tanto que estas entidades son responsables del tratamiento de los datos de sus clientes, les competen idénticas obligaciones que las señaladas hasta ahora para las operadoras referidas al cumplimiento del RGPD y la LOPDGDD, y además las derivadas del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

En efecto además de la remisión a la normativa de protección de datos que realiza el artículo 65 a cuyo tenor "*El tratamiento y cesión de los datos relacionados con las actividades a las que se refiere este real decreto-ley se encuentran sometidos a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la normativa española de protección de datos, y en la normativa nacional que lo desarrolla*" debe tenerse en cuenta la regulación específica del artículo 68 que bajo la denominación "Autenticación" señala lo siguiente:

> *1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante:*
>
> *a) acceda a su cuenta de pago en línea;*
>
> *b) inicie una operación de pago electrónico;*
>
> *c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.*
>
> *2. En lo que se refiere a la iniciación de las operaciones de pago electrónico mencionada en el apartado 1, letra b) respecto de las operaciones remotas de pago electrónico, los proveedores de servicios de pago aplicarán una autenticación reforzada de clientes que incluya elementos que asocien dinámicamente la operación a un importe y un beneficiario determinados.*
>
> *3. En los casos a los que se refiere el apartado 1, los proveedores de servicios de pago contarán con medidas de seguridad adecuadas para proteger la confidencialidad y la integridad de las*

credenciales de seguridad personalizadas de los usuarios de los servicios de pago.

4. Los apartados 2 y 3 se aplicarán asimismo cuando los pagos se inicien a través de un proveedor de servicios de iniciación de pagos. Los apartados 1 y 3 se aplicarán asimismo cuando la información se solicite a través de un proveedor de servicios de pago que preste servicios de información sobre cuentas.

5. El proveedor de servicios de pago gestor de cuenta permitirá al proveedor de servicios de iniciación de pagos y al proveedor de servicios de pago que preste servicios de información sobre cuentas utilizar los procedimientos de autenticación facilitados al usuario de servicios de pago por el proveedor de servicios de pago gestor de cuenta de conformidad con los apartados 1 y 3 y cuando intervenga el proveedor de servicios de iniciación de pagos, de conformidad con los apartados 1, 2 y 3.

Y define la autenticación y la autenticación reforzada en los siguientes términos:

Autenticación: procedimiento que permita al proveedor de servicios de pago comprobar la identidad de usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario.

Autenticación reforzada de cliente: la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes –es decir, que la vulneración de uno no compromete la fiabilidad de los demás–, y concebida de manera que se proteja la confidencialidad de los datos de identificación.

Es decir, “algo que sólo el usuario sabe” (como podrían ser un código PIN o una contraseña), “algo que el usuario tiene” (como podría ser una tarjeta de coordenadas o un teléfono móvil) y “algo que el usuario es” (como serían la huella, el rostro, la voz o el iris). Mediante la autenticación de doble factor, al comprobarse la identidad del usuario a través de dos mecanismos distintos, se añade un plus de seguridad a la operación electrónica.

Se establece así no solo la obligación de una autenticación reforzada para realizar una operación, sino que también para acceder al servicio de banca.

Es decir, la estafa del SIM Swapping requiere la vulneración de al menos dos *capas de seguridad,* la de la propia identificación y la de la operación en si misma considerada.

Por eso las entidades incluidas en el artículo 2 del citado RDLey, deben establecer todas las medidas necesarias para que la identificación y la autenticación sea eficaces de modo que impidan o dificulten la comisión de este tipo de fraudes, no correspondiendo a esta Agencia controlar dicha aplicación sino solo aquellas derivadas del cumplimiento del RGPD, a las que se ha hecho referencia en el apartado anterior.

XI

De acuerdo con lo expuesto cabe concluir en relación con el tratamiento de datos personales derivado de la persecución del SIM Swapping por parte de las FCS y el Ministerio Fiscal lo siguiente:

En primer lugar debe indicarse que si bien la STJUE de 8 de abril de 2014, Asunto C-293/2012 invalidó la *Directiva 2006/24/CE de 15 de marzo de 2006,* por la falta de proporcionalidad que podía suponer la aplicación de sus disposiciones, el Tribunal Supremo en Sentencia núm. 727/2020 de 23 de marzo deja claro que las deficiencias advertidas en la ciada Directiva no se producen en el actual ordenamiento jurídico nacional, y recuerda la plena vigencia de la Ley 25/2007 de 18 de octubre y su coexistencia con los preceptos de la LECrim.

Por lo tanto, el acceso a la información sobre el IMEI y el IMSI resultaría conforme a derecho en los cumpliendo los requisitos indicados en la citada normativa, ya estén vinculados a un proceso de comunicación, o simplemente persigan la identificación de su titular al margen de dicho proceso de comunicación.

En segundo lugar, y en relación con lo anterior, el acceso por parte de las FCS y el Ministerio Fiscal a los datos referidos a la vinculación entre el IMEI del dispositivo dónde se usa la SIM duplicada y la propia SIM salvo **mejor criterio de aquellos organismos o instituciones con competencias en este ámbito, no requerirá autorización judicial siempre y cuando la petición no esté vinculada a un proceso de comunicación concreto, en cuyo caso, se aplicaría la Ley 25/2007 de 18 de octubre.**

En tercer lugar, el tratamiento de datos personales de los afectados consistente en la comunicación por parte de las operadoras a las FCS y al Ministerio Fiscal de información sobre **las circunstancias de la solicitud de duplicado de la tarjeta SIM y su activación**, en el marco de una investigación por la comisión de delitos, se encuentra amparado con carácter general, desde el lado de las operadoras en el artículo 6.1 c) del RGPD, y una vez que la información obre en poder de las FCS y/o del Ministerio Fiscal, se encuentra amparado en la *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*, todo ello de conformidad con lo dispuesto en el artículo 588 ter m) de la LECrim.

En cuarto lugar, debe indicarse que la operativa técnica en que se produzca dicha comunicación, en relación con el acceso condicionado por el modo o manera en que las operadoras de telecomunicaciones almacenan los datos de tráfico son cuestiones ajenas a la competencia de la Agencia Española de Protección de Datos.

Y por último debe indicase que corresponde a las operadoras de telecomunicaciones y a las entidades bancarias **cumplir lo dispuesto en el RGPD en tanto responsables del tratamiento de los datos de sus clientes, y en especial establecer medidas para que el tratamiento sea leal, confidencial y se impida el acceso no autorizado por terceros a información personal**, de acuerdo con lo indicado en los artículos 5.1f), 24 y 32 del RGPD, y 28.2 de la LOPDGDD, sin perjuicio de lo que corresponda a las entidades bancarias como proveedores de servicios de pago derivado del *Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.*