CAPACIDADES DE ACTUACIÓN DEL MINISTERIO FISCAL Y LA POLICIA JUDICIAL TRAS LA REFORMA PROCESAL OPERADA POR LA LEY ORGÁNICA 13/2015: EN ESPECIAL LA OBTENCIÓN DE DIRECCIONES IP Y MUMERACIONES IMEI E IMSI (LOS APARTADOS K) A M) DEL ART. 588 TER DE LA LECRIM).

David Calvo López.

Fiscal Delegado de Delincuencia Informática de la Fiscalía Provincial de Almería.

Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid, 16 y 17 febrero de 2017.

*SUMARIO: 1. **INTRODUCCIÓN.** 2. **CONSIDERACIONES PREVIAS DE CARÁCTER GENERAL**.* 2.1 LA LEY ORGÁNICA 13/2015. MEDIDAS RESTRICTIVAS DE DERECHOS FUNDAMENTALES. 2.2. EL CONCEPTO DE "PROCESO DE COMUNICACIÓN". 2.3. LA LLAMADA "EXPECTATIVA RAZONABLE DE PRIVACIDAD". 2.4 DATOS DE TRÁFICO: CONCEPTO Y EVOLUCIÓN NORMATIVA DE SU PROTECCIÓN. **2.4.1 Definición y ámbito de datos de tráfico. Concepto diferenciado de datos de abonado. 2.4.2 Evolución de la normativa reguladora de la cesión los datos de tráfico. 3. CAPACIDAD DE INVESTIGACIÓN TECNOLÓGICA POR EL MINISTERIO FISCAL Y LA POLICÍA JUDICIAL SIN RECABAR AUTORIZACIÓN JUDICIAL.** 3.1. INTRODUCCIÓN. 3.2 OBTENCIÓN DE DIRECCIONES IP SIN AUTORIZACIÓN JUDICIAL: 588 TER K) LECRIM. 3.2.1 Formas de obtener la IP: ***3.2.1.1 La IP obtenida a través del Ciberpatrullaje; 3.2.1.2 Aportación por la víctima; 3.2.1.3 Hallazgos casuales; 3.2.1.4 Supuestos de urgencia; 3.2.1.5 Cesión mediante autorización judicial; 3.2.1.6 El problema de la "cesión voluntaria", sin previo requerimiento***. 3.3 IDENTIFICACIÓN DE TERMINALES MEDIANTE LA CAPTACIÓN DEL NÚMERO IMEI O IMSI: 588 TER L) LECRIM. **3.3.1 Conceptos tecnológicos básicos. 3.3.2 Utilidad práctica en las investigaciones tecnológicas. 3.3.3 La STS de 20 de mayo de 2008.** 3.4 IDENTIFICACIÓN DE TITULARES, TERMINALES O DISPOSITIVOS DE CONECTIVIDAD: 588 TER M) LECRIM. **3.4.1 Cuestiones generales. 3.4.2 Problemática de la aplicación del art. 588 ter m) de la LECrim. El Dictamen de la Fiscalía de Criminalidad Informática.**

RESUMEN:

En la investigación de los delitos cometidos a través de las TICs se va a producir de forma prácticamente ineludible la afectación de los derechos contenidos en el artículo 18 de la Constitución Española. En unas ocasiones la averiguación del delito y su autor exigirán tener conocimiento del contenido de la comunicación (artículo 18.3 CE) y en otras resultará invadido –en mayor o medida- únicamente el derecho a la intimidad (18.1) o a la protección de los datos personales (18.4 CE) mediante la cesión por parte de las entidades custodiantes de los mismos.

La regla general de esta cesión –establecida ya en la Ley 25/2007 de Conservación de Datos y ratificada por el artículo 588 ter j LECrim, introducido por LO 13/2015- es la necesidad de previa autorización judicial.

Sin embargo, al amparo de lo previsto en los apartados k) a m) del art.588 ter LECrim, dicho requisito no es exigible a las investigaciones de Policía Judicial y Ministerio Fiscal si se trata de obtener la IP de una comunicación ilícita cuando se trata de un dato público de la Red. Tampoco requiere de habilitación judicial el uso por las fuerzas policiales de artificios técnicos que permitan captar etiquetas técnicas o códigos de identificación de un terminal de telecomunicaciones (como el IMEI o el IMSI). Finalmente, los llamados "datos de abonado" también deberán ser facilitados directamente a los agentes investigadores en la medida de que se trata de información desconectada de un proceso comunicativo concreto, circunstancia que los hace merecedores de un menor grado de protección.

1.INTRODUCCIÓN.

Las innovaciones tecnológicas han trasformado nuestra realidad tan profundamente que podemos hablar de un mundo virtual paralelo que ha cambiado nuestra forma de socializarnos, tanto en el ámbito de nuestras relaciones personales, como en las económicas o de cualquier otro ámbito.

Gracias a los nuevos medios de comunicación, dos personas que no han coincidido jamás en tiempo y espacio, salvo el virtual, se pueden conocer, enamorar e iniciar una relación. También es verdad que, gracias al poder que nos otorgan esos mismos medios informáticos, en caso de ruptura y desavenencias graves de la pareja, su uso indebido permiten adentrarnos en poco tiempo hasta los últimos rincones de la intimidad ajena buscando causar el máximo daño posible.

Otro tanto ocurre en las relaciones comerciales. El llamado Comercio Electrónico está suponiendo, cada vez con mayor habitualidad, la sustitución de la actividad en las tiendas o locales de negocios mercantiles por la interacción de las partes contratantes a través de la Red.

Las operaciones mercantiles en Internet gozan de la gran ventaja de que el número de personas a las que se dirige el ofrecimiento de compra o venta es enormemente superior al de los procedimientos tradicionales, lo cual ofrece grandes posibilidades a los agentes económicos. El problema es que este tipo de negocios da pie a innumerables fraudes amparos en la impunidad que proporciona el relativo anonimato del usuario telemático.

En definitiva, el mundo virtual no es sino reflejo del mundo real y prácticamente todos los hechos delictivos que se pueden cometer tienen ya o tendrán, en un futuro no muy lejano, una modalidad informática.

Si a esto añadimos que nuestras normas penales van siempre por detrás de la realidad social, la metamorfosis sufrida fruto de la aparición de los fenómenos informáticos -que supone la irrupción constante de modalidades delictivas hasta entonces desconocidas- obliga al legislador a reaccionar revisando constantemente los tipos penales (especialmente los más clásicos) ante la evidencia de que existen lagunas por cubrir.

Igualmente cambian las formas de investigarlos. Las normas previstas en nuestra anciana Ley de Enjuiciamiento Criminal del año 1882 y sus escasas reformas - a pesar del esfuerzo jurisprudencial por reinterpretarlas- no se adaptaban al siempre exigible deber de previsión legal que amparase la actuación de las Fuerzas y Cuerpos de Seguridad, Ministerio Fiscal y Jurisdicción ordenada a la obtención de pruebas válidas para conseguir el descubrimiento del hecho criminal y acreditar la identidad de la autoría del mismo.

Este déficit de previsión normativa es el que viene a subsanarse con la LO 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.

2. CONSIDERACIONES PREVIAS DE CARÁCTER GENERAL.

2.1. LA LEY ORGÁNICA 13/2015. MEDIDAS RESTRICTIVAS DE DERECHOS FUNDAMENTALES.

En la investigación de la delincuencia que se sirve como instrumento de las nuevas tecnologías será necesario, en muchas ocasiones, adoptar medidas que afecten a derechos y libertades del ciudadano sospechoso. Por ese motivo y al amparo de lo previsto en el artículo 81.1 de nuestra Carta Magna, el desarrollo normativo relativo a estas diligencias probatorias se ha producido con rango de Ley Orgánica.

Esta invasión tecnológica será necesaria no solo para esclarecer el hecho delictivo en sí–que no siempre estará perfectamente definido al iniciarse las pesquisas-, sino también y sobre todo para averiguar la identidad de su autor. Uno de los fines de la instrucción (art 299 LECrim) es precisamente determinar la filiación de los presuntos autores de un ilícito, siendo esta tarea especialmente compleja en la materia que nos ocupa debido al uso de "nicks", influencia de virus troyanos, uso por un colectivo indeterminado del mismo terminal, así como otras argucias y trabas que, conforme iremos viendo a lo largo de nuestra exposición, dificultan enormemente la tarea de las Fuerzas y Cuerpos de Seguridad que investigan estos delitos.

Los derechos fundamentales afectados son principalmente los recogidos en el art 18 de la CE[1]:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

En cuanto al alcance de lo que debe entenderse por "*secreto de las comunicaciones*" debemos hacer referencia a la *Sentencia del Tribunal Constitucional 123/2002, de 20 de mayo* en que otorga el amparo al recurrente porque la entrega por la compañía telefónica a la Policía de los listados de llamadas del investigado no contaba con la preceptiva autorización judicial. Con cita de la simbólica sentencia 114/1984 del mismo Tribunal, así como de la sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984 (caso Malone), declaraba que: "*el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores*".

Igualmente, sin dejar lugar alguno a la duda, enumeraba el contenido que integra el derecho fundamental:

[1] Como normativa supranacional debemos citar el artículo 8 del Convenio Europeo de Derechos Humanos; la Carta de Derechos Fundamentales de la Unión Europea (artículo 7) y el artículo 12 de la Declaración Universal de Derechos Humanos y Pactos Civiles y Políticos de 1948, así como el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966.

"…garantiza a los interlocutores o comunicantes la confidencialidad de la comunicación telefónica que comprende el secreto de la existencia de la comunicación misma y el contenido de lo comunicado, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino; y ello con independencia del carácter público o privado de la red de transmisión de la comunicación y del medio de transmisión –eléctrico, electromagnético u óptico, etc...– de la misma."

Por otra parte, hoy en día en casi inconcebible un ser humano que no maneje con cierta asiduidad dispositivos electrónicos para sus necesidades más cotidianas. De dicha práctica se deriva, de forma directa o indirecta, tal cantidad de información y datos del perfil del usuario que podemos hablar de la aparición un nuevo derecho fundamental, la "*protección del propio entorno virtual"* (*STS, Sala 2ª, de 10-3-2016*):

"Es por ello por lo que el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual".

"Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital".

Evidentemente, toda esa información no es igual de sensible y en algunos casos, como los meros datos de abonado o registro para disfrutar de un servicio digital, no podemos hablar de que resulte afectado el secreto comunicativo, por lo que no se les dispensa la misma protección ni garantías legales, en especial el acceso exclusivo mediante autorización judicial.

Esto es trascendental a la hora de determinar el régimen jurídico de su cesión por la entidad custodiante del dato a las Fuerzas y Cuerpos de Seguridad, puesto que en ocasiones la ley permitirá la obtención directa de la información apartándose del principio general de que tengan que ser habilitados por un Juez.

De esos supuestos excepcionales a dicha regla general contenida en la Ley 25/2007 de Conservación de Datos y ratificada por el artículo 588 ter j) LECrim, recientemente introducido por LO 13/2015, tratará nuestra exposición.

2.2. EL CONCEPTO DE "PROCESO DE COMUNICACIÓN".

Ya hemos visto que el artículo 18.3 CE protege el contenido de las comunicaciones, al cual solo se puede acceder previa autorización judicial.

También hemos hecho referencia a que determinados datos que en sí mismos no constituyen el secreto de la comunicación, en la medida en que revelan la identidad de los interlocutores u otras circunstancias externas igualmente relevantes (momento, duración o destino) son merecedores del mismo amparo que el núcleo duro del derecho fundamental.

Esos datos, conocidos como de tráfico y que estudiaremos con profundidad más adelante, solo pueden obtenerse de las operadoras de telecomunicaciones o empresas prestadoras del servicio comunicativo correspondiente previa autorización judicial.

En cualquier caso, es importante destacar que tanto el art. 588 ter j) LECrim como la propia Exposición de Motivos de la LO 13/2015 se encargan de precisar que ese régimen

privilegiado solo viene referido a los supuestos en que esos datos vayan asociados a un "*proceso de comunicación*". Por lo tanto, debemos analizar a qué se refiere el legislador con esa expresión.

El concepto de "comunicación" es susceptible de interpretarse en el sentido más amplio como "comunicación electrónica" y ésta se produce tanto en las relaciones interpersonales (mandamos un email, hacemos una llamada o entablamos una conversación con otros semejantes en un foro) como incluso en las conexiones entre máquinas (un teléfono móvil "interactúa" con la antena que le presta servicio).

Sin embargo, nos parece más plausible restringir el alcance del término a las relaciones entre seres humanos. Siguiendo en este punto a ZARAGOZA TEJADA[2], deberían excluirse los supuestos de transmisión de señales entre entes de carácter impersonal o ajenos al "trato o correspondencia entre dos o más personas" (una de las acepciones de la Real Academia Española de la Lengua).

Por lo tanto, en caso de investigar la IP asociada a un anuncio[3] cuya única finalidad es servir de anzuelo para una estafa en masa, o en el caso de subir el usuario a la red un archivo que contiene pornografía infantil, la cesión por parte de la entidad que tutela el dato no exigiría autorización judicial por no afectar a un proceso comunicativo.

En la misma línea, RODRÍGUEZ LAINZ[4] concluye que la Constitución no protege, bajo el amparo del secreto comunicativo, el diálogo automático generado entre máquinas para su gobernanza, quien además destaca que tanto la Circular 1/2013 de la Fiscalía General del Estado como reciente jurisprudencia[5], circunscriben la titularidad de dicho derecho a los seres humanos.

En resumen, sin intercambio de ideas, datos o cualquier tipo de información entre dos o más seres humanos, no cabe hablar de comunicación. Y sin comunicación, no se puede pretender el amparo del artículo 18.3 de nuestra Constitución.

2.3. LA LLAMADA "EXPECTATIVA RAZONABLE DE PRIVACIDAD".

El acceso al secreto comunicativo y a los datos de tráfico que acompañan al mismo se puede producir también mediante el consentimiento expreso o tácito del titular del derecho. Para describir en qué supuestos puede considerarse que la inmisión es inconsentida, la jurisprudencia atiende a la posible vulneración de la "expectativa razonable de privacidad".

Cuando le cedemos a un amigo o familiar nuestro ordenador para su uso personal, o cuando lo depositamos en un establecimiento para su inspección profesional–pensemos en el

---

[2] Zaragoza Tejada, Javier Ignacio. "La investigación de la dirección IP tras la reforma operada por ley 13/2015". Aranzadi, número de febrero 2017.

[3] En la práctica, con Oficio policial y tras informar del atestado instruído, se está obteniendo de páginas web como "mil anuncios" la información sobre la IP de subida de ese anuncio, la cuenta de correo electrónico asociada al mismo, así como todos los anuncios publicados a través de esa cuenta de correo.

[4] Rodríguez Lainz, Jose Luis. "Análisis del Espectro Electromágnético de Señales Inalámbricas: rastreo de dispositivos Wi-fi-2. Diario la Ley: Año 2015, Número 8588.

[5] Ver STC 170/2013, de 7 de octubre, STC 281/2006, de 9 de octubre o la STS 766/2008, de 27 de noviembre.

famoso caso de la STC 173/2011 relativa al técnico que recibe un terminal para su reparación y acaba descubriendo pornografía infantil- el acceso a la intimidad del titular se ha producido en virtud de su propio consentimiento.

En ocasiones, dicha autorización será expresa. En otras, la mayoría, deberemos deducirla de los actos de abandono del titular, poniendo la información indiscriminadamente a disposición de terceros.

Si almaceno fotografías, publico informaciones o hago comentarios en mi perfil de FACEBOOK y, voluntariamente o por mera ignorancia de cómo funciona la configuración de privacidad, no excluyo a los usuarios que no tengo agregados como contactos de confianza, luego no podré sentirme defraudado en mis expectativas de confidencialidad.

Si interacciono con otras personas a través de una red de intercambio de archivos P2P, no debo luego extrañarme si terceros obtienen fácilmente información sobre la IP que tengo asignada, puesto que esos datos pasan a ser de "dominio público" por la misma dinámica del sistema que estoy utilizando.

Sirve también de ejemplo para la idea que trato de describir el cuerpo jurisprudencial que se ha elaborado en relación a la fiscalización empresarial del correo electrónico corporativo de sus empleados contenido en las resoluciones *STC 241/2012 de 17 diciembre, STC 170/2013 de 7 octubre o STS, Sala de lo Social, de 8 de marzo de 2011*.

En la STC 170/2013, el Alto tribunal avala que las empresas puedan vigilar el correo electrónico corporativo de sus trabajadores. No existe vulneración de la intimidad ni del derecho al secreto de las comunicaciones del empleado por cuanto se trata de un correo corporativo, para el cual tanto el Estatuto de los Trabajadores -como en su caso el propio convenio sectorial- admiten dicho control con el fin de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

La resolución atribuye especial trascendencia al hecho de que la inspección empresarial del correo corporativo leído y almacenado en el disco duro del terminal informático propiedad de la empresa no se hace mediante mecanismos de interceptación de los correos electrónicos en tiempo real, sino cuando el proceso de comunicación podía entenderse ya finalizado. Y de ello extrae la conclusión, en relación eso sí con el poder de inspección del empresario, de que la actuación de éste *"...no ha supuesto una interceptación o conocimiento antijurídicos de comunicaciones ajenas realizadas en canal cerrado"*.

La STC 241/2012, claro precedente tenido en cuenta por la anterior, concluye que los sistemas informáticos de la empresa son un instrumento de trabajo sujeto a las facultades de control del empresario sobre sus empleados. Y esa inspección puede venir referida no solo a las comunicaciones ya finalizadas por parte de los usuarios, sino también a otros aspectos íntimos como el historial de navegaciones en Internet.

Sin embargo, es fundamental para que no se vulnere el derecho a la intimidad del trabajador que por el empresario se haga expresa y clara advertencia sobre los límites de utilización del correo corporativo y de la posibilidad de realizar controles al efecto sobre cualquier herramienta tecnológica puesta a su disposición por motivos laborales (así se deduce de la STS 8-3-11, Sala de lo Social).

En definitiva, cuando concurren todas estas condiciones, el acceso por parte del empresario a esos correos no puede considerarse que vulnera la "expectativa razonable de intimidad" de los trabajadores.

2.4 DATOS DE TRÁFICO: CONCEPTO Y EVOLUCIÓN NORMATIVA DE SU PROTECCIÓN.

La regulación en nuestro sistema procesal penal en lo relativo a la intervención de las comunicaciones telemáticas, así como el acceso a los llamados datos de tráfico, ha sido extremadamente pobre por no decir inexistente hasta la reciente reforma introducida por LO 13/2015.

Dicho vacío legal se ha venido cubriendo gracias a normas extrapenales y a una abundante jurisprudencia que trataba de estirar y aplicar extensivamente las escasas normas sobre intervenciones telefónicas, postales y telegráficas (arts. 579 y ss LECrim) al resto de modalidades comunicativas que iban surgiendo con la revolución tecnológica.

2.4.1 Definición y ámbito de datos de tráfico. Concepto diferenciado de datos de abonado.

Cuando se establece una comunicación telemática, la información viaja agrupada de forma estandarizada en "unidades" que contendrán no solo el mensaje trasladado, sino también los datos de origen, destino y ruta del mismo, así como otros necesarios para la prestación y facturación del servicio por la empresa facilitadora.

Esta información sobre el origen y destino, que no constituyen el objeto del mensaje sino su trayectoria, es la que se conoce como "datos de tráfico".

La segunda categoría a la que denomina la doctrina "datos de abonado" se almacena en los registros de quien presta el servicio a efectos de posibilitar su ejecución así como con finalidades contractuales con el cliente. Aunque esta información también suele viajar junto con el mensaje principal cuando se establece la comunicación, generalmente podrá obtenerse de forma independiente a la misma.

El concepto de "dato de tráfico" viene dado por el Convenio de Ciberdelincuencia del Consejo de Europa de Budapest, de 23 de noviembre de 2001:

"*…cualquier dato informático relativo a la comunicación por medio de sistema informático, generado por el sistema informático que forma parte de la cadena de comunicación, indicando origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente*".

El mismo Convenio, en su artículo 18.3 define lo que debemos entender por "datos de abonado", que evidentemente en ningún caso comprenderán los datos sobre el tráfico o el contenido:

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

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

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".

Las consecuencias jurídicas de considerar un dato como "de tráfico" o como "de abonado" es sustancial, puesto que los primeros han sido asimilados por ley y jurisprudencia a los de contenido –y por lo tanto están protegidos por el 18.3 CE- y los de abonado forman parte del derecho a la autodeterminación informativa del 18.4 CE. El acceso a estos últimos no vendría condicionado por la necesidad de previa autorización judicial si se reclaman por la fuerza instructora policial en el seno de una investigación delictiva.

Habrá que plantearse, tal y como señala la *Circular 1/2013 de la FGE,* de entre todos los datos de tráfico generados y externos al contenido mismo de la comunicación, cuáles contienen información tan íntimamente ligada al secreto de lo comunicado que también merezca idéntica protección. Los restantes no encontrarán amparo en el artículo 18.3 de la Carta Magna, sino en el derecho a la protección de datos que se regula por la LOPD 15/1999 y que encuentra previsión constitucional en el artículo 18.4 CE.

Sí que estarían incluidos, como señala la citada Circular 1/2013 FGE, aquellos "datos accesorios pero íntimamente ligados a la propia comunicación" por revelar el origen y destino de la misma, su momento y duración y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Son, en definitiva, datos que se generan mientras la comunicación se encuentra en curso.

En el mismo sentido debemos destacar la *STS de 18 de marzo de 2010, nº247/2010*, puesto que hace una distinción fundamental para resolver cualquier cuestión relativa a los derechos amparados por el artículo 18 CE. Una cosa son los datos personales que afectan al secreto de las comunicaciones y otra bien distinta aquellos que, sin estar referidos a una concreta comunicación, se conservan y tratan como datos estáticos por las operadoras que se hallan obligados a la reserva frente a terceros:

"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)".

La propia LO 13/2015, que reforma nuestra Ley de Enjuiciamiento Criminal, también aporta valiosa información para terminar de delimitar conceptos. Así, el artículo 588 ter b) LECrim exige que la resolución judicial habilitante precise el contenido de la intervención de las comunicaciones telemáticas, que puede venir referido a tres conceptos distintos: a) el mensaje comunicado; b) los datos electrónicos de tráfico o asociados al proceso de comunicación y c) aquellos producidos con independencia del establecimiento o no de una concreta comunicación:

"La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con

independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario".

Y la propia norma aporta un concepto de lo que debemos entender por "datos electrónicos de tráfico o asociados":

"A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga"

Por lo tanto, al margen del hiperprotegido artículo 18.3 CE quedarían los "datos de abonado" (de la persona física o jurídica registrada para disfrutar del servicio). También los "datos de conexión" relativos a la identificación de un abonado o de un concreto terminal (IMSI e IMEI).

Estos datos se generan, frente a los de la categoría privilegiada, bien antes de la comunicación (datos de abonado o de registro), bien cuando ésta ha finalizado (a efectos de facturación). En este mismo nivel habría que incluir aquellos datos que se generen simultáneamente a la misma comunicación, pero que puedan ser obtenidos con independencia a la misma.

Todos estos datos conservados por las operadoras de telecomunicaciones a efectos de prestación y facturación del servicio, son los que pueden obtenerse por las Fuerzas y Cuerpos de Seguridad del Estado oficiando directamente y sin necesidad de mandamiento judicial.

Para ello se encuentran amparados por la reformada Ley de Enjuiciamiento Criminal y las facultades de prevención y averiguación del delito que le otorgan sus normas de actuación, así como la propia LO 15/1999, de 13 de diciembre, de Protección de Datos (especialmente su artículo 22).

2.4.2 Evolución de la normativa reguladora de la cesión de datos de tráfico.

Como hemos comentado con anterioridad, para la investigación de cualquier delito telemático resulta primordial acceder a datos personales de toda índole del investigado (médicos o bancarios, p.ej) y por supuesto, también los específicos generados como consecuencia de sus comunicaciones electrónicas.

Para ello, contábamos únicamente con la LO 15/1999 de Protección de Datos, los dictámenes de su Gabinete Técnico[6] y diversa normativa accesoria que permitía a las fuerzas

[6] El Gabinete Jurídico de la Agencia Española de Protección Datos ha tenido ocasión de pronunciarse favorablemente sobre la cesión directa de datos a las FFCCs en varias ocasiones. Concretamente, debemos destacar dos dictámenes:

a) *Informe 213/2004*, sobre cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad. Concluye, tomando como base el artículo 22.2 LOPD, que la entidad custodiante del dato puede comunicarlo a la Policía sin necesidad de mandamiento judicial ni consentimiento del titular del mismo en los casos en que la propia entidad presente una denuncia.

b) *Informe 297/2005*, en este caso autorizando la cesión por parte de las empresas de telecomunicaciones de los datos contractuales de sus abonados, a fin de que por los mismos pueda procederse a la realización de las investigaciones que sean necesarias para el esclarecimiento de hechos presuntamente delictivos.

policiales acceder, en determinados casos y sin autorización judicial, a dicha información reservada.

Para regular una materia tan específica dentro de la categoría general de los "datos personales", trasponiendo la Directiva 2006/24/CE del Parlamento Europeo y del Consejo[7], nació la *Ley 25/2007, de 18 octubre, de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*.

Esta ley, de forma tajante en sus artículos 1º y 6º, exige la correspondiente autorización judicial para la cesión de los datos conservados que se enumeran en el artículo 3 de la norma a los agentes facultados (FFCCs, Vigilancia Aduanera y CNI).

La ley 25/2007 vino en definitiva a endurecer las condiciones establecidas por la LOPD de cesión de datos a las fuerzas policiales, siempre y cuando fuesen relativas a las comunicaciones electrónicas y redes públicas de comunicaciones.

El problema que se planteaba por el inferior rango normativo de la norma posterior (la Ley 25/2007 es ley ordinaria), queda solventado al tener la reforma 13/2015 de la LECrim la categoría de Ley Orgánica, exigiendo el artículo 588 ter j) –como el 6 de la LCD- el requisito de la preceptiva autorización judicial para la cesión de datos.

En cualquier caso, tanto la Exposición de Motivos de la LO 13/2015 como el propio 588 ter j) LECrim, restringen la necesidad de que la cesión de datos venga avalada por resolución judicial a aquellos supuestos en que se trate de "*datos vinculados a procesos de comunicación*"[8]. Sensu contrario, se podrá acceder sin dicho condicionante por parte de la Policía Judicial a la información que se genere de forma independiente a los mismos:

EXPOSICIÓN DE MOTIVOS LO 13/2015: "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"

Artículo 588 ter j Datos obrantes en archivos automatizados de los prestadores de servicios

"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".**

[7] Anulada por STJUE de fecha 8 de abril 2014 por no garantizar suficientemente la protección y seguridad de los datos, ni asegurar la proporcionalidad necesaria para su cesión, vicios de los que no adolece nuestra ley nacional. Precisamente el hecho de que la cesión de datos venga supeditada en nuestra ley de Conservación a una previa autorización judicial, es uno de los baluartes para defender su vigencia a nivel de Derecho interno, con independencia de la suerte corrida por la normativa europea que fue traspuesta.

[8] Así lo destaca Huete Nogueras, José Javier en "La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados". Número 2 de la Revista del Ministerio Fiscal. 2016.

3. CAPACIDAD DE INVESTIGACIÓN TECNOLÓGICA POR EL MINISTERIO FISCAL Y LA POLICÍA JUDICIAL SIN RECABAR AUTORIZACIÓN JUDICIAL.

3.1 INTRODUCCIÓN.

Las Fuerzas y Cuerpos de Seguridad en general y sus brigadas de Policía Judicial, en particular, tienen como misión garantizar la seguridad ciudadana, hacer averiguaciones acerca de los responsables y circunstancias de los hechos delictivos, así como recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial.[9]

La investigación de delitos informáticos, a diferencia de la persecución de otro tipo de infracciones, requiere en ocasiones de un alto grado de conocimientos tecnológicos que los operadores jurídicos, aún reconociendo su conveniencia, no están obligados a tener. Por ese motivo, en la mayoría de ocasiones, es la fuerza policial especializada encargada de la averiguación de los hechos quien va proponiendo al Juez instructor las diligencias que deben acordarse para el esclarecimiento de los mismos.

En ese juego de propuestas, mandamientos y requerimientos, se va en ocasiones un tiempo muy valioso si tenemos en cuenta el alto grado de volatilidad de las pruebas telemáticas y la caducidad -12 meses desde su producción[10]- en el deber de conservar los datos generados por comunicaciones electrónicas que tienen las empresas proveedoras de estos servicios.

Por todo ello, es fundamental determinar el grado de autonomía de que disponen las Fuerzas y Cuerpos de Seguridad en sus investigaciones tecnológicas, tanto propias como las que se desarrollan bajo las directrices del Ministerio Fiscal.

También sería importante tener en cuenta, a efectos de futuras regulaciones normativas de la materia, la conveniencia de conceder mayores facultades a los investigadores policiales para dotar de agilidad sus pesquisas, sin tener que acudir al juez en aquellos supuestos en que sea tangencial la afectación del derecho fundamental. Para ello habría que ampliar, consecuentemente, su habilitación legal.[11]

En cuanto al Ministerio Fiscal, fundamentalmente son dos las normas habilitantes de sus investigaciones preprocesales: el artículo 773.2 LECrim y el artículo 5 de su Estatuto Orgánico.

Cuando el Ministerio Público tenga conocimiento de un hecho presuntamente delictivo, incoará este tipo de diligencias tendentes a comprobar si efectivamente tiene encaje en un tipo legal. En caso afirmativo, interpondrá la correspondiente denuncia o querella, judicializando el

---

[9] Así se recoge, entre otras muchas normas, en el artículo 104 CE; LOPJ (art 549.1.a); LO 2/1986 (art. 34.2); LOPD 15/1999 (artículo 22.2) o más recientemente, la LO 4/2015 de 30 de marzo, de protección de la seguridad ciudadana.

[10] Artículo 5 de la Ley 25/2007, de 18 octubre.

[11] A idéntica conclusión habría que llegar también en una hipotética instrucción dirigida por el Ministerio Fiscal con la figura de un "juez de garantías". De hecho y para que sirva de ejemplo, en el Borrador del Código Procesal Penal, en los artículos 311 y 312, se recogía la necesidad de que pasaran por el Ministerio Público, previamente a su ejecución, las iniciativas policiales de usar artificios para captar el IMSI o el IMEI, así como la petición al Juez de garantías de solicitar información en relación con una IP a la que han tenido acceso en sus investigaciones.

asunto. En el supuesto contrario, archivará sus actuaciones comunicándoselo al denunciante por si desea proporcionar la "notitia criminis" a un órgano jurisdiccional, cuya valoración no tiene por qué coincidir con la del Ministerio Público.

Las limitaciones son evidentes teniendo en cuenta, sobre todo, que solo podrá realizar aquellas diligencias para las que esté legitimado según la LECrim, "*las cuales no podrán suponer la adopción de medidas cautelares o limitativas de derechos*"(art 5.2 EOMF). Y en el ámbito de las investigaciones tecnológicas, caracterizadas por la afectación del artículo 18 CE, esas condiciones le dejan muy poco recorrido antes de su judicialización.

3.2 OBTENCIÓN DE DIRECCIONES IP SIN AUTORIZACIÓN JUDICIAL: 588 TER K) LECRIM.

En cualquier investigación tecnológica relacionada con el uso de Internet, un dato básico para avanzar en las pesquisas será la IP[12] asociada a la comunicación ilícita. Una vez obtenida –posteriormente veremos en qué casos se puede conseguir de forma autónoma por la fuerza policial-, habrá que dirigirse a la empresa de telecomunicaciones que se la asignó al usuario para que nos desvele quién es el abonado que se corresponde con la misma. Esta última petición, en la medida en que sirve para identificar al interviniente, tendrá que formalizarse mediante autorización judicial.

Siguiendo la línea ya trazada por la Ley 25/2007, el artículo 588 ter k) LECrim establece lo siguiente en lo relativo a la identificación mediante número IP:

"Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión de algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso".

Con una IP y el nombre del abonado a quien se le asignó, ya tenemos un sospechoso. El problema vendrá después para vincular el equipo informático con un usuario determinado, el presunto autor del delito telemático, puesto que no siempre quien aparezca formalmente como titular de la línea será el autor material de la actividad ilícita. Para ello deberán realizarse las pesquisas tradicionales al igual que en otro tipo de comunicaciones. Evidentemente y por poner un ejemplo sencillo, el titular de un teléfono no siempre es el responsable de las llamadas amenazantes que se realizan desde él, por lo que deberá averiguarse qué persona física, de entre todas las que han tenido acceso a ese terminal, fue la que hizo uso del mismo un día y una hora en concreto.

Son muy numerosas las posibilidades de autoencubrimiento y ocultación de que dispone el delincuente informático, de manera que es bastante frecuente que logre el anonimato y por tanto la impunidad de sus operaciones.

---

[12] Internet Protocol, compuesto por cuatro bytes o grupos de números naturales, que pueden adquirir el valor 0 hasta 255, separados entre sí por puntos. Estos dígitos permiten un número aproximado de 4000 millones de combinaciones, es decir, identificar a 4000 millones de equipos informáticos diferentes conectados a Internet en un momento dado. Este número es asignado por el proveedor ISP al usuario cuando empieza a usar el servicio y es el que permite su identificación.

Pensemos en la instalación de troyanos, uso de proxies o técnicas de anonimización como la navegación a través de la red TOR. Desgraciadamente, también es frecuente que la investigación tecnológica llegue a un punto muerto al descubrirse que la IP está ubicada en el extranjero, pertenece a un Cibercafé o a cualquier centro público con múltiples e indeterminados usuarios o, simplemente, pertenezca al wifi de un incauto vecino cuya conexión no había encriptado.

Otro de los problemas que se están encontrando los investigadores telemáticos es la creciente tendencia por los administradores a ocultar la IP pública en las cabeceras técnicas de los correos electrónicos. Es una práctica que se está extendiendo y que entorpece aún más la actividad policial, cercenando sus ya de por si menguadas capacidades de actuar sin tener que recurrir a la autorización judicial.

También debemos hacer mención a las IP "tipo NAT"[13] a las que cada vez con más frecuencia se recurre por las operadoras debido a la tremenda demanda de usuarios que se quieren conectar simultáneamente a Internet.

Resumidamente, consiste en hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP pública. Esto permite a grandes empresas usar una sola dirección IP y no tantas como máquinas estén conectadas y también se usa para conectar redes domésticas a Internet.

Antes, como a cada persona el ISP le asignaba una IP con la que navegaba, bastaba con deshacer el camino recorrido para identificar al usuario cuando cometía un delito. Ahora con la misma IP puede haber cientos o miles de usuarios simultáneamente conectados (mismo día, hora y segundo).

Cuando se implementa un sistema tipo NAT, es la IP púbica a la que llegamos con nuestra investigación, configurándose como una especie de subred o red intermedia. Al solicitar a las operadoras de telecomunicaciones que identifiquen al usuario, como se han conectado múltiples clientes con ella (a los que se les asigna una IP privada dentro de esa red local) nos requerirán para que les facilitemos información adicional (que normalmente será el puerto de conexión y ese dato no siempre está a nuestra disposición).

En definitiva, cada vez es más complicado obtener el dato IP directamente y sin necesidad de solicitar su cesión.

[13] Network Address Translation (Traducción de Direcciones de Red).

3.2.1 Formas de obtener la IP: a) como dato público disponible para cualquier internauta, b) aportación por la víctima, c) hallazgos casuales, d) supuestos de urgencia, e) cesión mediante autorización judicial y f) el problema de la "cesión voluntaria", sin previo requerimiento.

3.2.1.1 La IP obtenida a través del Ciberpatrullaje.

Las Fuerzas y Cuerpos de Seguridad, velando por la seguridad de los internautas y amparados en la normativa que regula su actividad, desarrollan continuamente rastreos y sondeos de red con fines preventivos o de investigación.

Como algunas de las herramientas utilizadas para localizar archivos ilícitos no están exentas de críticas[14], la jurisprudencia se ha encargado de validar la obtención por parte de los agentes policiales de datos electrónicos públicos, por ejemplo cuando se usan sistemas de intercambio de archivos P2P, siendo el más conocido el programa EMULE.

En estos supuestos nos encontramos ante información accesible para cualquier usuario, no precisándose de autorización judicial para conseguir lo que es público y ha introducido en la red el propio investigado.

Entre otras muchas,[15] la *STS 842/2010 de 7 de octubre, Ponente Sr Colmenero Menéndez de Luarca*, entiende regular la actuación policial:

"…los rastreos que realizan en estos casos los agentes policiales tienen por objeto desenmascarar la identidad tríptica de los IPs que habían accedido a los "hush" que contenían pornografía infantil. El acceso a dicha información, calificada por el recurrente de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma".

"Consecuentemente, quien utiliza un programa P2P asume que muchos d el os datos que él mismo incorpora a la red con su actividad se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía no se hallaban protegidos por el artículo 18.1 ni por el 18.3 CE".

La huella de la entrada queda registrada y ello lo sabe o debe conocer el usuario, que no puede alegar la más arriba mencionada "*expectativa razonable de privacidad*", por lo que esta información no encuentra amparo en el artículo 18 CE.

En caso de denuncias de usuarios que se han descargado accidentalmente un archivo de pornografía infantil, nada impide a los agentes averiguar el código hash del fichero e identificar los "nicks" e IP de conexión de los usuarios que se lo estaban bajando o que lo tenían en su carpeta compartida.

Para saber a qué proveedor en concreto hay que dirigirle el Oficio para que identifique quién es el titular de la línea asociado a esa IP, también disponemos de bases de datos públicas

[14] Véase Cabezudo Rodríguez, Nicolás en "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal". Boletín del Ministerio de Justicia, número 2186. Febrero 2016.

[15] STS 17-11-2011, 680/2010 o 739/2008, entre otras.

conocidas como "*whois*", por lo que dicha información está disponible para ser usada no solo por las Fuerzas y Cuerpos de Seguridad, sino también para cualquier usuario de Internet.

A partir de ahí ya se puede y debe judicializar la investigación para saber quién es el abonado al que se adjudicó esa IP y practicar la entrada y registro para ocupar el sistema informático, diligencias ambas que requieren de autorización judicial.

3.2.1.2 Aportación de la IP por la víctima.

Imaginemos que una persona recibe un correo electrónico mediante el cual se le extorsiona y que en la cabecera técnica del mismo aparece la IP del remitente. Cuando acude a interponer la correspondiente denuncia aporta toda la información de la que dispone para facilitar la identificación del autor de los hechos.

¿Se puede usar lícitamente ese dato en la investigación? Por supuesto que sí. En primer lugar, porque el denunciante es parte en ese proceso comunicativo, por lo que puede disponer de los datos principales y accesorios al mismo[16].

Además, sería un dato de tipo público introducido con todas las consecuencias en la red de telecomunicaciones por el atacante, por lo que de nuevo afirmamos que no se puede amparar en unas expectativas razonables de privacidad.

Lo mismo, aunque de forma más clara y evidente, ocurre si recibo una llamada amenazante desde un teléfono móvil. El número emisor de la llamada es un dato propio y totalmente disponible para la víctima que puede y debe ceder a la Policía.

3.2.1.3 Los hallazgos casuales

Imaginemos que alguien recibe por error una carta de la que no era destinatario en su buzón. Y que, sin ser consciente de dicha circunstancia, abre el sobre descubriendo un contenido ilícito. Esto mismo podría ocurrir con un correo electrónico, estando visible el dato de la IP del remitente.

Imaginemos también que alguien lleva a reparar su ordenador a una tienda especializada y el técnico del establecimiento, en el desarrollo de sus labores para atender el encargo del cliente, encuentra entre los archivos almacenados en el terminal pornografía infantil.

¿Qué ocurre en esos casos? Si esos ciudadanos que se han encontrado con la información íntima que aparenta ser un hecho ilícito lo comunican a la Policía en cumplimiento del deber general de denunciar delitos públicos recogido en los artículos 259 y 262 LECrim, esa prueba, así obtenida, ¿es válida o nula por vulneración de un derecho fundamental?

Este tipo de supuestos han sido resueltos tanto por el Tribunal Supremo como por el Tribunal Constitucional, decantándose por la licitud de la prueba puesto que no se trata de injerencias voluntarias en la intimidad o secreto comunicativo ajeno:

"En consecuencia, mal puede hablarse de prueba ilícita a partir del análisis de la forma en que las imágenes y demás contenidos accedieron a la causa. No deben incluirse en ese concepto los descubrimientos efectuados de forma casual por un ciudadano - en este caso, el hallazgo del técnico al que fue encargada la

[16] Un compendio de resoluciones en este sentido, especialmente de nuestro Tribunal Constitucional, puede encontrarse en la Circular 1/2013 FGE, apartado 5.2, páginas 22 a 25.

reparación del ordenador- que, en el momento de su obtención, carece de toda voluntad de hacerse con una fuente de prueba. Es evidente que no puede obtener el mismo tratamiento jurídico la accidental apertura de un sobre introducido por error en un buzón que no es el de su destinatario -equivocación que permite el descubrimiento de un hecho de relieve penal-, frente a la fractura intencionada del buzón de un vecino con la finalidad de acceder a su correspondencia y vulnerar así su intimidad" (STS 4-12-2015, nº 786/2015)

Además, en los casos de entregar a un tercero nuestro dispositivo electrónico que contiene almacenados los datos sensibles, habilitándole para su uso (personal a un amigo o profesional, como el caso del técnico que tiene que reparar un ordenador) podemos hablar de consentimiento expreso o tácito:

"... el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 ; 196/2006, de 3 de julio , FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio , FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto «aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida» (SSTC 196/2004, de 15 de noviembre, FJ 2 ; 206/2007, de 24 de septiembre, FJ 5 ; 70/2009, de 23 de marzo , FJ 2). En lo relativo a la forma de prestación del consentimiento, hemos manifestado que este no precisa ser expreso, admitiéndose también un consentimiento tácito. Así, en la STC 196/2004, de 15 de noviembre , en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconocimos no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9). También llegamos a esta conclusión en las SSTC 22/1984, de 17 de febrero y 209/2007, de 24 de septiembre , en supuestos referentes al derecho a la inviolabilidad del domicilio del art. 18.2 CE , manifestando en la primera que este consentimiento no necesita ser «expreso» (FJ 3) y en la segunda que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito (FJ 5) "(STCo 173/2011, de 7-11-2011).

Tal y como señala VELASCO NÚÑEZ[17] estos supuestos son equiparables a la entrega de información por la víctima, siempre y cuando la obtención de la misma se haya producido de buena fe.

3.2.1.4 Obtención de IP en supuestos de urgencia.

El artículo 588 ter d) apartado 3, estrictamente para los *delitos de terrorismo o en los que intervengan bandas armadas*, permite cuando así lo exijan razones de urgencia que sea el propio Ministro del Interior (en su defecto el Secretario de Estado de Seguridad) quien ordene la interceptación de las comunicaciones tanto telefónicas como telemáticas, con obligación de comunicarlo al juez competente con carácter inmediato y, en todo caso, en el plazo máximo de veinticuatro horas.

Lo excepcional debe interpretarse restrictivamente. La autoridad ordenante será el Ministro del Interior o el Secretario de Estado de Seguridad, pero sin duda la iniciativa y propuesta de tan urgente medida provendrá de los agentes policiales encargados de la investigación.

Aunque no lo diga expresamente el apartado citado, interpretado sistemáticamente junto con los anteriores del precepto, así como las previsiones de la sección y capítulo en que se

[17] Velasco Núñez, Eloy, en su obra "Delitos Tecnológicos: definición, investigación y prueba en el proceso penal (Ed. Sepin, 2016), páginas 86 y 87.

contiene, es razonable concluir que esta situación excepcional es extensible a los supuestos en los que se pretende la cesión de datos[18].

Partiendo de la máxima de "quien puede lo más, puede lo menos", carecería de sentido el que, por razones de urgencia, se pueda acceder a los contenidos y, sin embargo, queden fuera de tal posibilidad los datos de tráfico como la IP.

En la misma línea justificativa por la urgencia de la actuación policial, también debemos hacer mención al art 588 sexies c) apartados 3 y 4 sobre ampliación del registro de dispositivos de almacenamiento masivo de información u observación directa de datos siempre que se "*aprecie un interés constitucionalmente legítimo que haga imprescindible la medida*".

En estos casos se accede por parte de los agentes actuantes y sin autorización judicial a información asociada al derecho fundamental protegido, aunque inmediatamente después deba ser convalidada su actuación.

3.2.1.5 Cesión mediante autorización judicial: la ley de Conservación de Datos 25/2007.

La IP, conforme al artículo 3 de la Ley 25/2007 es uno de los datos que los prestadores de servicios están obligados a conservar. En la medida en que este dato, unido a otros de los que han procesado las operadoras, puede servir para identificar a un usuario o un determinado dispositivo de conectividad, su incorporación al proceso entraría dentro del ámbito de la necesaria autorización judicial (artículo 6 de la ley).

Esta norma marca un antes y en el régimen legal de la cesión de la IP a las fuerzas policiales e incluso al Ministerio Fiscal. Además, la exigencia como norma general de la cesión de datos de tráfico mediante autorización judicial viene confirmada por el artículo 588 ter j) LECrim.

Especialmente significativa es la *STS de 18 de marzo de 2010, nº247/2010*. En el supuesto estudiado, el Alto Tribunal convalidó la petición directa por la Fiscalía –basándose en la normativa de la LOPD 15/1999, artículo 11.2 d)- a la empresa proveedora de servicios de todos los datos que permitieran identificar a la persona a la que se adjudicó una IP.

No obstante, el tribunal marca una línea roja y solo admite la validez de la actuación porque se produjo antes de entrar en vigor la normativa sobre Conservación de Datos. Después de la misma, es ineludible para obtener la cesión de dicha información contar con la preceptiva autorización judicial, incluso para el Ministerio Fiscal tal y como se recoge en el acuerdo del *Pleno no jurisdiccional de 23 de febrero de 2010*:

"Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Mº Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007 de 18 de octubre".

[18] A esta conclusión llegan también Marchena Gómez, Manuel y González-Cuéllar Serrano, Nicolás en "La reforma de la Ley de Enjuiciamiento Criminal en 2015", Castillo de Luna Ediciones Jurídicas, 2015, pp. 223, así como Ríos Pintado, Juan Francisco en "La reforma procesal. Incorporación de Datos de Tráfico". Jornadas de Especialistas en Criminalidad Informática, 2016. Disponible en página web del CEJ.

Por lo tanto, debemos distinguir por un lado los casos de rastreo policial del espacio público y por otro los supuestos en los que para acceder a una información sobre la IP es necesario oficiar a una operadora.

En este último supuesto, según concluye la reforma procesal introducida en nuestra LECrim por LO 13/2015, sí debe recabarse previamente autorización judicial, siguiendo la línea marcada por la Ley 25/2007 o reiterados pronunciamientos judiciales como las SSTS nº 292/2008 de 28 de mayo, 236/2008 de 9 de mayo o la 680/2010 de 14 de julio, así como por la Circular 1/2013 FGE, sobre intervención de comunicaciones telefónicas.

Igualmente, incluso si hemos obtenido la IP de forma independiente, necesitaremos también de dicha habilitación judicial para requerir de las operadoras los datos que permitan identificar al usuario, terminal o dispositivo de conectividad asociado a la misma por así establecerlo el artículo 588 ter k) LECrim.

3.2.1.6 El problema de la "cesión voluntaria", sin previo requerimiento.

Como bien es sabido, cada vez son más frecuentes los excesos verbales de determinados usuarios cuando hacen comentarios a una noticia que se ha subido a la edición digital de un periódico o revista.

Para investigar los hechos que no encuentren encaje en el legítimo uso de la libertad de expresión, será necesario normalmente pedir los datos de abonado o registro del usuario que ha hecho la comunicación ilícita.

El problema se plantea cuando el medio digital, requerido directamente por la Policía Judicial o el Ministerio Fiscal en el seno de unas diligencias de investigación del artículo 5 EOMF, proporciona sorpresivamente, sin haberles requerido para ello, la IP asociada a la conexión mediante la cual se subió el comentario a la noticia.

¿Qué hacemos con ese dato? ¿Lo utilizamos o mejor lo obviamos hasta que no haya una resolución judicial que requiera al medio para que lo aporte a la investigación? La cuestión no es baladí, puesto que una nulidad probatoria en cadena produciría fatales consecuencias en el resultado del proceso.

Adelantamos que, desde nuestro punto de vista, la incorporación de la IP así aportada a la investigación se realizaría *contra legem* debido al claro y tajante tenor de la Ley de Conservación de Datos y el artículo 588 ter j) LECrim, puesto que se trata de un dato conexo a un proceso de comunicación.

Además, como la interpretación de estos preceptos debe ser restrictiva – a favor del investigado, puesto que afecta a sus derechos fundamentales- no podemos hacer una aplicación extensiva de los mismos. La ley 25/2007 tan solo prevé una "cesión rogada" de estos datos, sin que exista previsión alguna del supuesto de "entrega de oficio" o "voluntaria" de los mismos por parte de la entidad custodiante.

A continuación, trataremos de justificar nuestra postura. Lo haremos de forma resumida puesto que las ideas que se van a exponer se remiten a todos los conceptos que hemos desarrollado con anterioridad en este estudio:

1) Como adelantábamos, el artículo 588 ter j) LECrim exige que, para la cesión de datos obrantes en archivos automatizados de los prestadores de servicios, se

reclamen en virtud de resolución judicial siempre que "*se encuentren vinculados a procesos de comunicación*". Cuando se trata de un mensaje vertido en la sección de comentarios a noticias digitales, en una red social o en cualquier otro supuesto en el que interactúas con otros usuarios, estamos hablando de un acto de comunicación entre dos o más personas.

2) El citado artículo señala entre los destinatarios del deber de colaboración a los "prestadores de servicios". Y estos medios de comunicación digitales tienen a todos los efectos dicha consideración.[19]

3) El periódico digital no es un tercero que se encuentra con esa IP de forma casual o fortuita. La conoce como administrador de ese foro fruto de una relación de contractual con el cliente, donde tiene la potestad de eliminar comentarios inapropiados e incluso bloquear la IP de un usuario. Los prestadores de servicios acceden a ese dato en el desarrollo de sus funciones administrativas de gestión y tienen el deber legal de conservarlo. Su cesión, por lo tanto, también se debe producir conforme a la ley que establece un principio general claro y tajante: la necesaria autorización judicial.

4) Tampoco es comparable este supuesto al de la víctima que recibe una comunicación delictiva y denuncia los hechos proporcionando todos los datos que tiene para facilitar la identificación del autor. El que participa de una conversación no se ve afectado por el secreto de la misma, pero el periódico digital aquí no tiene la condición de interviniente sino de administrador en la prestación de un servicio digital.

5) Cuando la IP no puede ser obtenida por los agentes investigadores de forma directa (dato público rastreado en la red), tienen que pedir a las entidades prestadoras de servicios que se los cedan. Y eso solo es posible previa autorización judicial porque así lo exige la ley. Cabría aplicar en este caso la doctrina jurisprudencial de la "*expectativa razonable de privacidad*".

6) El propio Convenio de Ciberdelincuencia de Budapest explica lo que debe entenderse por dato de tráfico y dato de abonado. Sin duda la IP de subida del mensaje comunicado, en la medida en que viene referido al origen del mismo, pertenece a la primera categoría.

7) Del estudio conjunto de las Directivas Europeas, la evolución jurisprudencial nacional y supranacional, así como de nuestra ley de Conservación de Datos (artículo 6), se deduce una voluntad inequívoca de que los datos de tráfico generados con motivo de una comunicación están protegidos, de manera que solo pueden cederse con previa autorización judicial o previo consentimiento del afectado.

8) Acudiendo al concepto recogido en el artículo 3 LOPD, apartado h), es *consentimiento del interesado toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".* En este caso no lo hay, ni expreso ni tácito,

[19] Incluso el apartado II de la Exposición de Motivos de la ley 34/2002, de 11 de julio, los pone como ejemplo de lo que está incluido en un concepto amplio de "servicios de la Sociedad de la Información".

salvo que convalide el internauta esta posibilidad de cesión no requerida al aceptar las condiciones generales cuando se registra como usuario en el periódico digital (por lo que hemos podido comprobar, no se suele recoger esta cláusula en el pliego).

9) Es cierto que una IP no conduce directamente a una persona, pero el artículo 3 de la LOPD 15/1999 define "*dato de carácter personal*" como cualquier información concerniente a una persona física "*identificada o identificable*". Por su parte, el Real Decreto 1720/2007 que desarrolla la referida Ley Orgánica, precisa todavía más el término al referirlo a "*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*".

10) Normalmente, no concurrirán razones de urgencia que impidan acudir al juez para obtener el mandamiento judicial. Situación distinta sería si alguien publica en un foro una información creíble relativa a un inminente atentado terrorista. En esos casos, ya hemos visto que los agentes pueden solicitar colaboración directa al administrador para la urgente identificación del usuario. Sin embargo, incluso para estos supuestos especiales, no está prevista legalmente la cesión voluntaria de esa información por parte del prestador del servicio.

En conclusión, lo más prudente en este supuesto sería no hacer uso de esa IP que nos proporciona el medio digital sin permiso judicial ni consentimiento de su titular y, preventivamente al amparo del artículo 588 octies LECrim, ordenar la conservación de datos para que los retengan a disposición de la investigación mientras se obtiene la autorización para su cesión.

3.3 IDENTIFICACIÓN DE TERMINALES MEDIANTE LA CAPTACIÓN DEL NÚMERO IMEI O IMSI: 588 TER L) LECRIM.

El artículo 588 ter l) de la LECrim, regula la identificación de los terminales o tarjetas usadas por el investigado mediante captación de códigos del aparato o de sus componentes:

1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.

El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Aunque nuestra exposición se va a centrar en el IMEI y el IMSI, por así destacarlos el precepto, no dejan de ser dos ejemplos dentro de una lista abierta. En este sentido e interpretando el art. 588 ter l) LECrim, debemos destacar la recientísimas *STS 967/2016 de 21 de diciembre y 551/2016 de 22 de junio* que convalidan la obtención por la Policía Judicial del número PIN de una Blackberry sin previa autorización judicial. Concluyen estas resoluciones

que se trata tan solo de un código que da acceso al terminal telefónico, sin que resulte afectado el secreto de las comunicaciones.

Para una adecuada comprensión del alcance y significado de este precepto, es necesario incorporar explicaciones técnicas de lo que es la numeración IMEI y la IMSI, así como hacer una serie de aclaraciones sobre su utilidad práctica en una investigación penal. Finalmente, debemos hacer expresa mención a la Sentencia del Tribunal Supremo de 20 de mayo de 2008, puesto que su doctrina avalando este tipo de prácticas policiales es la que finalmente adquiere rango normativo, encarnándose en el artículo 588 ter l) LECrim.

3.3.1 Conceptos tecnológicos básicos

Siguiendo en este punto, entre otras fuentes de información, la *Circular 1/2013 de la Fiscalía General del Estado* así como el *Informe de la Unidad Central de Delitos Informáticos* de la que hablaremos con mayor detalle en el siguiente punto de la exposición, debemos hacer las siguientes precisiones de tipo técnico:

Un dispositivo de comunicaciones móviles celulares -lo que coloquialmente llamamos teléfono móvil- se compone de dos elementos:

a) el terminal físico o equipo electrónico móvil

b) el módulo de identificación de usuario, conocido como tarjeta SIM *(Subscriber Identity Module*). Esta tarjeta SIM es intercambiable entre los diferentes terminales móviles y contiene en su chip digital la información necesaria para identificar y autenticar al abonado, incluido el número IMSI.

El **IMEI** *(International Mobile Equipement Identity*)[20] es un código que identifica inequívocamente a un determinado dispositivo móvil. Identifica el propio terminal físico con independencia de la tarjeta SIM que tenga introducida, la cual individualizará al abonado concreto que esté haciendo uso del terminal en cada momento[21].

El **IMSI** *(International Mobile Suscriber Identity*) es el código que identifica internacionalmente al abonado de una línea de comunicación móvil. Se trata de un código único que se integra en una tarjeta SIM y a partir del cual se asigna al usuario un número de abonado o MSISDN (Moblile Station Integrated Services Digital Network) que conocemos como número comercial.

La tarjeta inteligente SIM contiene una programación que, una vez introducido el PIN (personal identification number) permite la búsqueda de redes GSM y UMTS y trata de validarse en una de ellas. Una vez validado por la red, puesto que también es un sistema preventivo del fraude, el teléfono queda registrado y está disponible para usar los servicios contratados.

EL IMSI es por tanto fundamental para identificar al usuario del teléfono y aparece en todas las conexiones entre el terminal y la red. Esa interacción y el consiguiente trasvase de

[20] Cuya numeración puede comprobarse desde el propio teléfono marcando *#06#.

[21] En definitiva, viene a ser como el "chasis" del teléfono pero, por desgracia y aunque debería ser inalterable, también es suplantable. Si llevas tu teléfono a determinados establecimientos para que te lo liberen, puedes terminar perfectamente con un IMEI genérico. Se conecta el teléfono a una consola y se puede cambiar el IMEI. Es como alterar el bastidor de un coche, se lija el que hay y se pone otro.

datos se produce, por supuesto, cuando se está produciendo una conversación telefónica, pero no debemos olvidar que también hay conexión desde el momento en que se enciende el terminal, y por lo tanto en situaciones ajenas a un proceso comunicativo concreto[22].

Tanto el IMSI como el IMEI forman parte de los datos generados por la comunicación electrónica, concretamente las de telefonía móvil y se prevé como tal en el artículo 3 de la ley de Conservación de datos.[23] De interrelacionarse con el resto de información disponible para el operador de telecomunicaciones, puede lograrse la identidad del comunicante.

Sin embargo, solo cuando la obtención vaya ligada a un proceso comunicativo concreto puede considerarse merecedor el dato de una protección asimilada al del secreto mismo. En los casos de obtención independiente del dato, haciendo uso de los dispositivos técnicos apropiados, la Policía Judicial se encuentra legitimada en su actuación en virtud de lo dispuesto en el artículo 588 ter l) LECrim.

Es importante señalar por último que, tanto con el IMSI como con el IMEI, se dispone de información suficiente para solicitar la autorización judicial de intervención de las comunicaciones.

3.3.2 Utilidad práctica en las investigaciones tecnológicas.

Las nuevas tecnologías, en especial el extendido uso de teléfonos móviles, nos proporcionan una magnífica fuente de información para investigar cualquier delito, no solamente los telemáticos.

Si alguien comete un homicidio y en los momentos previos o posteriores al crimen ha hecho uso de su terminal móvil, esa información queda registrada y podremos comprobar las conexiones al repetidor más cercano.

En el caso de que alguien haya robado en varias poblaciones distintas, para los periodos de tiempo que nos interese, podemos pedir información sobre todos los abonados que se conectan a la antena más próxima y luego cruzar datos. Habrá seguramente un único IMSI que aparezca en todas las conexiones.

Como veremos más adelante, en los casos en que se sustrae a la víctima su terminal móvil (que tiene asignado un IMEI que lo identifica) es fundamental obtener información de las tarjetas SIM que se insertan en el mismo, puesto que nos permitirá asociar a unos abonados concretos con el teléfono sustraído.

Cuando los agentes necesitan conocer el número del que está haciendo uso un sospechoso, se puede servir de artificios técnicos para captar su IMSI. Para ello, aproximan disimuladamente (normalmente en un maletín) un escáner que simula el comportamiento de la red GSM y al que se conecta, transmitiendo su información identificativa, ese teléfono móvil.

---

[22] González López, J.J., apunta que, evidentemente, también puede obtenerse el dato con el terminal desconectado en el difícil supuesto de que se pueda incautar el mismo y mediante la inspección directa de la SIM en "*Obtención de la IMSI con fines de investigación penal. Comentario a la STS 249/2008*". Revista Jurídica de Castilla y León, nº 23, enero 2011, pág. 185

[23] Apartado e): Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación.

La operativa consiste en tomar varias muestras en diversos sitios significativos asociados al investigado (primero en la zona de su domicilio, después en la zona donde trabaja, luego en la zona donde disfruta de su ocio, etc…). y después se triangula la información. Primero se extraen todos los datos y luego se entrecruzan para que ver el único que es común a todos esos muestreos.

El artículo 588 ter l) LECrim se encarga de destacar –lo hace en dos ocasiones- que tanto la obtención del dato IMEI como del IMSI se tiene que producir en el marco de una investigación policial concreta. Esto supone descartar cualquier finalidad privada, pero desde luego tampoco se exige desde este momento tan inicial de las pesquisas que el hecho delictivo se encuentre perfectamente definido.

En la práctica esto supone la introducción a efectos de investigación policial de algunos de los principios generales del art. 588 bis a) LECrim –proporcionalidad, idoneidad, etc-, cuya observancia podrá ser comprobada por la autoridad judicial. De ahí que la solicitud posterior de intervención telefónica *"habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior".* Y dicha solicitud puede ser autorizada o denegada, valorando, entre otros motivos, la abusiva utilización de estos artificios técnicos (IMSI-catcher).

3.3.3 La STS 249/2008 de 20 de mayo de 2008.

El artículo 588 ter l) LECrim supone la plasmación legal de la doctrina del Tribunal Supremo establecida en la Sentencia de 20 de mayo de 2008, en la que se concluye que no es necesaria la autorización judicial para que las fuerzas de seguridad capten determinados datos técnicos del aparato emisor que usa un investigado.

Como comentamos en las cuestiones generales, los preceptos relativos a la investigación tecnológica que se regulan en la LECrim vienen a cubrir una laguna normativa y que hasta entonces se subsanaba con una abundante doctrina interpretativa jurisprudencial.

Precisamente las resoluciones del Tribunal Supremo, especialmente la *Sentencia 249/2008 de 20 de mayo, Ponente Excmo. Sr. Don Manuel Marchena Gómez*, habían concretado la naturaleza del dato IMSI y si debía ser encuadrado dentro de la esfera de especial protección del 18.3 CE cuando era captado por agentes de las fuerzas policiales sin autorización judicial.

En el caso concreto, uno de los recurrentes había planteado vulneración del referido derecho fundamental puesto que el IMSI fue captado directamente por la Guardia Civil, aunque posteriormente ya se solicitó autorización judicial para dirigirse a las compañías telefónicas para que identificasen los números de teléfono que se correspondían con esos IMSI y su consiguiente intervención.

La Sentencia considera que en virtud del artículo 6 de la ley 25/2007 e interpretando las Directivas Europeas, la *cesión* por el IMSI por las operadoras necesita autorización judicial previa. Pero también se plantea si la *captación autónoma* por las Fuerzas y Cuerpos de Seguridad afecta al derecho del 18.3 CE (secreto de la comunicación) o al núcleo duro de la privacidad, los llamados datos especialmente protegidos que tendrían acogida en el artículo 18.4 de la Carta Magna.

El alto Tribunal acaba amparando esta práctica policial basándose en el artículo 22, apartados 2 y 3, de la Ley Orgánica de Protección de Datos, cuyo tenor literal es el siguiente:

"2. 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.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales".

En definitiva, concluye la resolución que es precisa autorización judicial para la *cesión* del IMSI por las operadoras, pero su *obtención o captura* autónoma por las fuerzas de seguridad no afecta al secreto de las comunicaciones en cuanto que esa información por si sola no permite averiguar la identidad de los comunicantes, la titularidad del teléfono móvil o cualesquiera otras circunstancias que tienen ese especial amparo.

Para finalizar con este apartado, debemos hacer referencia a una de las apreciaciones de esta Sentencia, puesto que expresamente afirma que la captación autónoma queda validada pero es necesaria autorización judicial para solicitar el resto de información de que disponen las operadoras y que permiten identificar el número comercial del abonado:

"Para que la numeración IMSI brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa o, lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado. Los mismos agentes de Policía que hayan logrado la captación del IMSI en el marco de la investigación criminal, habrán de solicitar autorización judicial para que la operadora correspondiente ceda en su favor otros datos que, debidamente tratados, permitirán obtener información singularmente valiosa para la investigación. En definitiva, así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia".

Entendemos que esta afirmación debe interpretarse por la fecha en que se dicta la resolución, puesto que el artículo 588 ter m) LECrim –introducido por LO 13/2015- habilita en la actualidad claramente a los agentes para que soliciten de forma directa esos datos que permitan la total identificación. Lo comprobamos a continuación.

3.4 IDENTIFICACIÓN DE TITULARES, TERMINALES O DISPOSITIVOS DE CONECTIVIDAD: 588 TER M) LECRIM.

A diferencia de la situación regulada en el artículo 588 ter j) LECrim (cesión de datos asociados a un proceso comunicativo), el legislador ha querido dotar de autonomía al Ministerio Fiscal y la Policía Judicial en determinados supuestos poco invasivos para los derechos contenidos en el artículo 18 CE.

Por este motivo, el artículo 588 ter m) LECrim prescinde de la garantía del previo control judicial para la mera identificación de terminales o dispositivos de conectividad:

"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".

La propia Exposición de Motivos de la LO 13/2015 también deja meridianamente claro que esta norma está reservada para los supuestos en que este tipo de información se obtiene de forma independiente del proceso comunicativo concreto: *…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".*

3.4.1 Cuestiones generales.

Para muchas investigaciones policiales, el punto de partida suele ser un número de teléfono. En ocasiones interesará saber quién es el abonado al mismo y, en otras, conocer todos los números comerciales que tiene registrados una determinada persona.

Da igual que se trate de tráfico de drogas, estafas, corrupción de menores, etc. Casi siempre hay una llamada de un número de teléfono, un SMS o un whatsapp. Por ejemplo, si yo subo a una página de compraventa de objetos un anuncio porque deseo que contacten conmigo las personas que quieren adquirir mi producto, una forma sencilla, cómoda y práctica de conseguirlo suele ser un número de teléfono. Y cuando la Policía necesite conocer la titularidad del mismo y los datos necesarios para identificar al cliente, lo puede solicitar directamente a las operadoras de telecomunicaciones amparándose en el apartado m) del articulo 588 ter de la LECrim.

En muchas ocasiones los datos proporcionados serán reales, pero te puedes encontrar otros ficticios según la seriedad de la compañía admitiendo el registro, no siendo infrecuente que se logren registrar como auténticos pasaportes que realmente son mendaces o de terceras personas.

Cuando los teléfonos están asociados a identidades de ciudadanos nacionales, o extranjeros pero regulares, las gestiones suelen ser sencillas y fiables. Todo lo contrario ocurre cuando quien se registra es un irregular o tenemos sospechas de que se ha utilizado un pasaporte falso. En esos casos, los agentes investigadores se ven obligados a solicitar información al país correspondiente para que determinen si esa persona existe y para que aporten, en su caso, una copia legítima de su documentación.

La astucia y medios del delincuente también es capaz de llevar la investigación policial, a través de la titularidad de una línea telefónica, a un callejón sin salida. Por poner un ejemplo, en una investigación por extorsión en Almería y siguiendo el rastro del número telefónico desde el que se emitían todo tipo de amenazas, nos topamos con que la titular era la propia víctima. Después de hacer indagaciones por otras vías, se logró descubrir que el investigado, por el tipo de negocio que regentaba, disponía de un ordenador autorizado para activar tarjetas de teléfono, circunstancia que aprovechó para dar de alta una línea de teléfono a nombre de la denunciante (de la que disponía de todos sus datos por haber sido su empleada).

3.4.2 Problemática de la aplicación del art. 588 ter m) de la LECrim. El Dictamen de la Fiscalía de Criminalidad Informática.

En este punto final de nuestra exposición, tenemos que hacer referencia a una incidencia que se ha detectado relativa a la negativa de algunas operadoras a ceder al Ministerio Fiscal o

Policía Judicial, salvo que medie autorización judicial, algunos de los datos a los que se refiere el artículo 588 ter) LECrim.

De las *Actas del Comité Técnico de la Comisión Nacional de Coordinación de Policía Judicial* de fechas 15 de julio y 24 de noviembre de 2016 se desprenden las objeciones de las Compañías de Telefonía a facilitar los datos relativos a la identificación del titular o número de terminal.

Respecto del artículo 588 ter m) de la LECrim, las Compañías de Telefonía consideran que es aplicable:

• Cuando a partir de los datos de identificación del individuo se les solicita el número de la línea telefónica, el IMSI y el IMEI.

• Cuando a partir del IMSI de la línea telefónica se les solicita el número de la línea telefónica y los datos de identificación del titular.

• Cuando a partir del IMEI del terminal se les solicita el número de la línea telefónica y los datos de identificación del titular que consten en sus bases de clientes.

En cambio, las mismas Compañías consideran que cuando a partir del IMEI del terminal se les solicita el número de la línea telefónica, el IMSI y los datos de identificación del titular, y el terminal no ha sido adquirido de la operadora, el artículo citado no es aplicable por ser necesario extraer la información solicitada del procesamiento de comunicaciones.

Trasladada la cuestión a la *Comisión Nacional de los Mercados y la Competencia, en su informe de 19 de octubre de 2016*, da como respuesta a la consulta planteada las siguientes consideraciones:

"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."

Finalmente, por las fuerzas policiales se solicitó informe sobre esta cuestión a la *Unidad Central del Área de Especialización en Criminalidad Informática*, quien ha emitido un *Dictamen*[24] muy detallado que pasamos a resumir a continuación.

[24] El Dictamen se encuentra pendiente de que la Secretaría Técnica de la FGE se pronuncie sobre el mismo, por lo que sus conclusiones no pueden darse a día de hoy por cerradas y definitivas.

El Dictamen de la Fiscalía de Criminalidad Informática

Para la persecución de delitos contra el patrimonio en los que se ha desposeído a la victima de su teléfono móvil, es fuente fundamental –y en ocasiones casi única- de investigación conocer la tarjeta SIM o número IMSI con que se ha conectado el referido terminal, puesto que a partir del IMEI del aparato (que normalmente proporciona la propia víctima) es posible obtener información por esta vía de la persona o personas que lo están utilizando. En definitiva, quien introduce su tarjeta SIM en un teléfono sustraído (que tenemos identificado por el IMEI) en los días posteriores al hecho ilícito es un buen sospechoso de haber participado en el mismo, o como ocurre en muchas ocasiones, de ser autor de un delito de receptación a la par que testigo en lo relativo a la autoría de la infracción principal.

Como decíamos más arriba, se está produciendo la incidencia de la negativa de algunos de los operadores de comunicaciones radicados en España a facilitar directamente, sin autorización judicial, estas informaciones: a) con qué tarjetas está conectándose un determinado móvil (conocemos el IMEI pero no la SIM insertada con la que opera) y b) qué teléfono concreto es el que contiene la SIM (aquí se conocen los datos de tarjeta, pero no del terminal donde se ha introducido).

Esta negativa se produce aun cuando dicha información se solicite de forma aislada y por tanto desligada de cualquier otra información relacionada con posibles procesos de comunicación mantenidos desde el terminal especifico en el espacio temporal respecto del cual se solicitan datos.

El Dictamen trata de dilucidar si con dicha posición las operadoras de telecomunicaciones están vulnerando lo dispuesto en el art 588 ter m) LECrim y por lo tanto deben colaborar, bajo apercibimiento de incurrir en un delito de desobediencia. La conclusión es afirmativa.

La tarjeta SIM –que contiene el código IMSI- se le entrega por la compañía a sus abonados y es imprescindible su colocación en el terminal para disfrutar de los servicios contratados. Esa información de "abonado o cliente" siempre la va a tener a su disposición. También dispondrá del número IMEI que identifica el teléfono móvil si la misma operadora fue la que se lo facilitó a dicho abonado.

Sin embargo, el consumidor puede optar por adquirir el terminal donde va a insertar la SIM a esa misma empresa o cualquier otra. También será frecuente la situación en que el cliente usa varios terminales –con sus respectivos IMEI- insertando la misma tarjeta.

¿Por qué se oponen a facilitar esos datos las compañías de Telefonía? Las operadoras de telecomunicaciones alegan que en realidad sí que tienen acceso a esa información requerida, pero la misma solo pueden obtenerla a partir de los registros derivados de las conexiones con la red efectuadas y por lo tanto acudiendo a sus bases de datos que almacenan el tráfico cursado y que, conforme a la Ley 25/2007 de Conservación de Datos, necesitan para su entrega de autorización judicial.

La Fiscalía especializada, partiendo de la distinción entre dato de tráfico frente al de abonado que se traza en el Convenio Budapest sobre Ciberdelincuencia del Consejo de

Europa[25], asigna a los códigos de identificación IMEI e IMSI a la segunda categoría. Y son datos de abonado porque tienen por objeto la mera identificación del terminal físico y de usuario siempre que la solicitud se haga como información independiente y desvinculada de cualquier proceso comunicativo.

En resumen, siempre que los datos IMEI e IMSI se obtengan de forma desvinculada a un proceso comunicativo, deben catalogarse como "datos de abonados" y son de obligatoria cesión directa por las operadoras a la fuerza instructora policial. Ambos componentes identifican técnicamente un equipo móvil, sin necesidad de entrar al detalle más privado –y por tanto constitucionalmente protegido- de su uso concreto mediante procesos de comunicación.

Esta situación es la que permite su encaje en el artículo 588 ter l) LECrim, descartándose la disposición general del 588 ter j), que por su enunciado queda restringido a los supuestos en que los datos provengan de una concreta comunicación. No olvidemos que estos datos pueden obtenerse con la mera puesta en funcionamiento del dispositivo móvil, sin necesidad por tanto de que se establezca una comunicación interpersonal.

Finalmente, concluye el Dictamen, "*la forma en que los operadores de comunicaciones decidan controlar/almacenar esos datos no podría 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*".

[25] Se perfila el concepto de "datos de abonado" en el artículo 18.3 del Convenio, así como en el informe preparatorio del mismo. Los "datos de tráfico" asociados a una comunicación vienen definidos en el artículo 1 d).

BIBLIOGRAFÍA UTILIZADA.

- Cabezudo Rodríguez, Nicolás. "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal (LO 13/2015)". Boletín del Ministerio de Justicia, número 2186. Febrero 2016.
- González López, J.J. "Obtención de la IMSI con fines de investigación penal. Comentario a la STS 249/2008". Revista Jurídica de Castilla y León, nº 23, enero 2011.
- Huete Nogueras, José Javier. "La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados". Número 2 de la Revista del Ministerio Fiscal. 2016.
- Marchena Gómez, Manuel y González-Cuéllar Serrano, Nicolás. "La reforma de la Ley de Enjuiciamiento Criminal en 2015", Castillo de Luna Ediciones Jurídicas, 2015.
- Ríos Pintado, Juan Francisco. "La reforma procesal. Incorporación de Datos de Tráfico". Jornadas de Especialistas en Criminalidad Informática, 2016. Disponible en página web del CEJ.
- Rodríguez Lainz, Jose Luis."Análisis del Espectro Electromágnético de Señales Inalámbricas: rastreo de dispositivos Wi-fi-2. Diario la Ley: Año 2015, Número 8588.
- Velasco Núñez, Eloy. "Delitos Tecnológicos: definición, investigación y prueba en el proceso penal" (Ed. Sepin, 2016).
- Zaragoza Tejada, Javier Ignacio. "La investigación de la dirección IP tras la reforma operada por ley 13/2015". Aranzadi, número de febrero 2017.