Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia núm. 249/2008 de 20 mayo. Recurso de Casación núm. 10983/2007

RESUMEN

El Tribunal Supremo estima que la obtención del IMSI (Código de identificación único para dispositivos de telefonía móvil) mediante escáner por las Fuerzas y Cuerpos de Seguridad del Estado es legítima y para ello no es necesaria la autorización judicial. Una vez conocido el IMSI si es necesario pedir autorización judicial para conocer los números de teléfono que pertenecen a cada IMSI e intervenir las comunicaciones de esos teléfonos.

I. ANTECEDENTES

PRIMERO

El Juzgado Central de Instrucción número 4, instruyó Sumario número 4/2005, contra Gonzalo, Manuel; Paulino, Jose Ángel, Blas, Rogelio, Simón, Jose Francisco, Carlos Jesús, Luis Angel, Adolfo, Marí Jose, Daniel, y Eusebio y, una vez concluso, lo remitió a la Sala de lo Penal de la Audiencia Nacional (Sección Primera) que, con fecha 27 de junio de 2007, dictó sentencia que contiene los siguientes HECHOS PROBADOS:

"Las pruebas practicadas permiten estimar acreditados los siguientes HECHOS, QUE SE DECLARAN PROBADOS:

A lo largo del año 2003 Gonzalo, mayor de edad, con antecedentes penales, al haber sido condenado en Sentencia de 20.1195, firme el 18.03.96, por un delito de tráfico de drogas a la pena de 8 años y 1 días de prisión mayor, y declarado rebelde el 28.10.02 en la causa 15/99 de la Sección 4ª de la A. N. por un delito contra la salud pública, y Adolfo, mayor de edad, con antecedentes penales, al haber sido condenado en Sentencia de 17.04.95, firme el 18.03.96, por un delito de detención ilegal a la pena de 6 años de prisión, sirviéndose de los contactos que tenían en Sudamérica, empezaron a preparar una operación para importar a España una importe cantidad de cocaína, que había de ser transportada desde Colombia o Venezuela en barco, para posteriormente ya en las proximidades de las costas españolas o africanas, ser transbordada a otro buque que permitiese su aproximación a las costas gallegas, donde sería finalmente desembarcada, mediante lanchas de pequeño tamaño.

Para realizar esta operación estaban puestos de acuerdo con Blas, mayor de edad, cuyos antecedentes penales no constan, que era el que se encargaba de controlar la posición del barco, que habría de transportar la cocaína, manteniendo informados a Gonzalo y a Adolfo, de las fechas y puntos de contactos para transbordar la carga.

Además Gonzalo y Adolfo también estaban de acuerdo con Daniel, mayor de edad, con antecedentes penales, al haber sido condenado en Sentencia de 20203, firme el 30.12.2003, por delito de tenencia ilícita de armas a la pena de 1 año de prisión, y Eusebio, mayor de edad, que se encargaban de facilitarles la infraestructura consistentes en remolques y embarcaciones de pequeño calado, tipo planeadoras y zodiac, para llevar a cabo el desembarco, y una nave donde guardarlas.

Gonzalo se encontraba en busca y captura, y para poder realizar estas actividades sin ser descubierto se valía de Marí Jose, mayor de edad, sin antecedentes penales, y de Luis Angel, mayor de edad, sin antecedentes penales, conocido como Cachas, quienes le ayudaban en todo lo que éste les encomendaba, sabiendo que Gonzalo estaba preparando una operación para importar cocaína, así se encargaban de vigilar la

existencia de vehículos en las proximidades que pudiesen pertenecer a la Guardia Civil, de hacerle llegar teléfonos móviles, y otros efectos.

Marí Jose, de nacionalidad ecuatoriana, ejercía la prostitución en un club de alterne, antes de conocer a Gonzalo, con el que entabló una relación sentimental, actualmente ha regularizado su situación y trabaja como auxiliar en una clínica dental.

Gonzalo consiguió que personas cuya identidad no consta le elaborasen un DNI con los datos de David, y con su fotografía. El auténtico David era vecino de Adolfo, y Gonzalo logró hacerse con sus datos personales so pretexto de la venta de un coche.

Blas consiguió también que personas cuya identidad no consta le proporcionasen un DNI y un carnet de conducir con los datos de Matías, y con su fotografía.

A finales de 2003 los contactos con los proveedores y entre los miembros del grupo se intensifican ante la inminencia de la salida de la droga, aunque se fueron produciendo distintas dificultades que retrasaron la operación. El día 9 de febrero de 2004 Gonzalo llamó por el teléfono NUM000 a una persona no identificada, para decirle que tenía que darle una buena noticia, que al camión le dieron salida a primera hora de la mañana,...que el día que estaba puesto se recogerían ahí las piezas, para indicarle con ello que el barco con la cocaína ya había salido, y que se podría recoger el día establecido la carga.

Efectivamente en los primeros días del mes de febrero de 2004 el barco pesquero DIRECCION000, con número de registro NUM001, y pabellón de Belice, salió de un puerto de Panamá, con la siguiente tripulación:

Simón, Capitán;
Carlos Jesús, Jefe de máquinas;
Jose Ángel, 1º oficial;
Jose Francisco, marinero;
Paulino, maquinista;
Rogelio, marinero; y
Manuel, cocinero.

Todos los miembros de la tripulación sabían que la auténtica finalidad del viaje era transportar cocaína. Cuando el barco DIRECCION000 se encontraba frente a las costas de Venezuela, fue cargado con 217 fardos de cocaína, desde otras embarcaciones de pequeño tamaño que se le aproximaron, y con esa carga en su bodega inició la ruta a través del Atlántico hacia las coordenadas 10º N Longitud y 35º W, donde se debería de encontrar con el barco al que debía transbordar la cocaína.

El día 12 de febrero de 2004 miembros de la Unidad Central Operativa y del Servicio de Vigilancia Aduanera procedieron al abordaje y posterior aprehensión de la embarcación DIRECCION000, con número de registro NUM001, cuando se encontraba en aguas internacionales, en la posición 09º 58Ž N Longitud 035º 30ŽW. En el momento en que los miembros del Servicio de Vigilancia Aduanera, con el apoyo de miembros de la Guardia Civil, accedieron al barco DIRECCION000, este buque no enarbolaba pabellón alguno, una vez en el barco requirieron al capitán para que presentase la correspondiente documentación, y al constatar que presentaba Patente de Navegación de Belice, y que en la bodega había fardos similares a los utilizados para transportar cocaína, se solicitó a través de los Servicios Centrales de Vigilancia Aduanera del Plan Nacional Contra la Droga que se procediera a solicitar autorización de las autoridades de BELIZE para el abordaje, lo que se obtuvo sobre las 20 horas,

procediendo entonces a la inspección de la nave y a la detención de los tripulantes al descubrir la carga de 217 fardos con cocaína en la bodega.

La carga y los detenidos fueron trasladados al buque del Servicio de Vigilancia Aduanera, y el barco DIRECCION000 hubo de ser remolcado hasta Las Canarias, por su estado, presentando uno de los dos motores averiados y surgiendo durante el trayecto una vía de agua.

La sustancia aprehendida resultó ser cocaína, con un peso de 4.444,27 kilos, y una pureza del 69,4%. Su valor en el mercado ilícito hubiese alcanzado la suma de 138.395.456 euros.

Al llevarse a cabo el registro en el domicilio de Gonzalo, sito en CAMINO000 núm. NUM002, Maceiras Covelo, Ponteareas, se le ocupó una pistola marca STAR, semiautomática, calibre 380, en perfecto estado de funcionamiento, con número de serie borrado, con su cargador, y 21 cartuchos 9 m-m k, y 4 teléfonos móviles. Gonzalo disponía del arma, pese a carecer de licencia de armas, y de la guía de pertenencia. Esa pistola se la había tenido guardada Daniel, hasta que el 12 de diciembre de 2003 Gonzalo mando a Marí Jose, que encargase a Luis Angel recogérsela y llevársela.

En el registro del coche WHS, utilizado por Blas, se ocuparon anotaciones con claves, con distintas coordenadas, entre ellas 10º N 35 W, así como múltiples anotaciones de distintas cantidades. También se le ocupó una nota con el núm. de teléfono que utilizaba para llamar a Gonzalo NUM000.

En la nave propiedad del padre de Eusebio, sita en Ribeira-Oleiros, calle Subridos s/n, se ocuparon: una lancha neumática, zodiac, deshinchada, una planeadora colocada en un remolque con dos motores, otra planeadora colocada en un remolque cerrado, sin motores, pero preparada para llevar cuatro motores. Estas embarcaciones iban a ser utilizadas para el desembarco de la cocaína."

SEGUNDO

La Audiencia de instancia dictó el siguiente pronunciamiento:

"FALLO: En atención a lo expuesto y por la autoridad que nos confiere la Constitución española, HEMOS DECIDIDO:

Que debemos condenar y condenamos a:

Gonzalo como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad, con la circunstancia agravante de reincidencia, […]; como autor de un delito de tenencia ilícita de armas […]; y como autor de un delito de falsificación de documento oficial […]

Adolfo, como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Blas como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Eusebio como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Daniel como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad, […]; y como autor de un delito de tenencia ilícita de armas, con la agravante de reincidencia […]

Simón como autor de un delito contra la Salud Pública de sustancia que causa grave a la salud, en cantidad de notoria importancia, y perteneciendo a una organización […]

Carlos Jesús como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización […]

Jose Ángel como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Paulino como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Rogelio como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Manuel como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Jose Francisco como autor de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Luis Angel, como cómplice de un delito contra Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

Marí Jose como cómplice de un delito contra la Salud Pública de sustancia que causa grave daño a la salud, en cantidad de notoria importancia, y perteneciendo a una organización, siendo el hecho de extrema gravedad […]

TERCERO

Notificada la sentencia a las partes, se preparó recurso de casación […]

II. FUNDAMENTOS DE DERECHO DE INTERÉS

[…]

RECURSO DE Arturo

CUARTO

El primero de los motivos hechos valer por la defensa de Arturo, se articula con fundamento en los arts. 5.4 de la LOPJ y 852 de la LECrim, al estimar vulnerado el derecho fundamental al secreto de las comunicaciones acogido en el art. 18.3 de la CE.

La infracción de este derecho se habría originado como consecuencia de la utilización por la Guardia Civil, sin autorización judicial, de unos mecanismos de barrido que permiten obtener los números IMSI de las tarjetas de telefonía prepago empleadas para comunicarse con el recurrente.

El motivo no puede ser aceptado.

La determinación de si ha existido o no la vulneración constitucional que denuncia el recurrente, impone hacer algunas consideraciones previas que nos permitirán definir el verdadero significado del IMSI, sus características técnicas y su funcionalidad en el marco de las comunicaciones telefónicas. Sólo así estaremos en condiciones de delimitar el régimen jurídico de su captación y subsiguiente incorporación al proceso penal.

A) **El término IMSI es el acrónimo de International Mobile Subscriber Identity. Se trata de un código de identificación único para cada dispositivo de telefonía móvil, representado por una serie de algoritmos, que se integra en la tarjeta SIM y que permite su identificación a través de las redes GSM y UMTS. Proporciona una medida adicional de seguridad en la telefonía móvil y, sobre todo, facilita la prevención del fraude en la telefonía celular.**

A partir de esa descripción técnica, no parece existir duda alguna de que el IMSI integra uno de los diferentes datos de tráfico generados por la comunicación electrónica, en nuestro caso, la comunicación mediante telefonía móvil. Su configuración técnica y su tratamiento automatizado por parte del proveedor de servicios son absolutamente indispensables para hacer posible el proceso de comunicación.

Tampoco resulta cuestionable que la comunicación mediante telefonía móvil ha de encuadrarse en el ámbito de las llamadas comunicaciones en canal cerrado, caracterizadas por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación. En el presente caso, incluso, el empleo de tarjetas prepago -cuya adquisición, al menos por ahora, puede realizarse sin ofrecer datos precisos de identidad personal-, es bien expresivo del deseo de los comunicantes de mantener a toda costa el secreto de la comunicación.

En el actual estado de la jurisprudencia, **la necesidad de proteger la inviolabilidad de las comunicaciones, con independencia del formato en el que aquéllas se desarrollen, representa un hecho ratificado por numerosos precedentes**. Así, el Tribunal Constitucional ha afirmado que la especial protección que dispensa el art. 18.3 de la CE se produce "...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" (STC 123/2002, 20 de mayo). Aquel precepto "...contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas", pues es preciso caminar hacia "...un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos" (STC 70/2002, 13 de abril).

En la misma línea, esta Sala ha proclamado que "...el ámbito de protección de este medio de comunicación -la telefonía- no tiene limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse. No sólo la primitiva telefonía por hilos sino también las modernas formas de interconexión por satélite o cualquier otra señal de comunicación a través de las ondas se encuentran bajo la tutela judicial" (STS 137/1999, 8 de febrero). Más recientemente, la STS 130/2007, 19 de febrero, afirmó que"...el umbral de la garantía del derecho al secreto de las comunicaciones tiene carácter rigurosamente preceptivo. Por tanto, es el ordenamiento el que establece sus términos y su alcance mismo. Así, como espacio de intimidad garantizado al máximo nivel normativo, no podría quedar, y no queda, a expensas de la evolución de los avances de la técnica, lo que supondría un riesgo permanente de eventual relativización,

con la consiguiente degradación de lo que es una relevante cuestión de derecho a mero dato fáctico".

En consecuencia, a falta de autorización judicial, cualquier forma de interceptación del contenido de la comunicación verificada por telefonía móvil, incluida su modalidad de tarjeta prepago, determinaría una flagrante vulneración del derecho constitucional al secreto de las comunicaciones garantizado por el art. 18.3 de la CE, con la inevitable consecuencia de la nulidad probatoria sancionada por el art. 11 de la LOPJ.

En el presente caso, todas las conversaciones intervenidas lo fueron en virtud de autorización judicial. No sucedió lo propio con la captación del IMSI, obtenido por los agentes de la Guardia Civil mediante la utilización de un escáner en las proximidades del usuario. Una vez lograda aquella serie alfanumérica, se instó de los respectivos operadores -ahora sí, con autorización judicial- la identificación de los números de teléfono que se correspondían con esos IMSI y su consiguiente intervención.

B) A partir de esos datos, **resulta obligado plantearse si la numeración IMSI, ajena al contenido de la comunicación propiamente dicho, encierra una información adicional que, pese a su carácter accesorio, se halle tan íntimamente ligada al secreto de lo comunicado que también merezca convertirse en objeto de protección constitucional**. Como es sabido, la jurisprudencia constitucional, tomando como inspiración la STEDH de 2 agosto de 1984 -Caso Malone-, ha venido insistiendo en que la protección alcanza frente a cualquier forma de interceptación en el proceso de comunicación mientras el proceso está teniendo lugar, siempre que sea apta para desvelar, ya sea la existencia misma de la comunicación, el contenido de lo comunicado o los elementos externos del proceso de comunicación (cfr. SSTC 114/1984, de 29 de noviembre; 123/2002, de 20 de mayo; 137/2002, de 3 de junio; 281/2006, 9 de octubre. También, SSTS 1231/2003, 25 de septiembre y 1219/2004, 10 de diciembre).

La clave interpretativa ofrecida por la jurisprudencia del TEDH ha resultado decisiva para afianzar el espacio de exclusión del secreto de las comunicaciones, extendiendo su ámbito a esos otros datos externos que no tienen por qué trascender a terceros ajenos al proceso de comunicación. El problema radica, sin embargo, en que la solución ofrecida en el Caso Malone -tanto por su singularidad, como por el estado de los avances técnicos en la fecha en que aquélla fue pronunciada- sólo pudo referirse a algunos datos muy concretos relacionados con la técnica del recuento -open register o comptage-. En efecto, según se precisa en el apartado 56 de la mencionada resolución, el recuento consiste en "...el uso de un instrumento -un contador combinado con un aparato impresor- que registra los números marcados en un determinado aparato telefónico y la hora y la duración de cada llamada". Añade el Tribunal de Estrasburgo que "...el recuento es distinto por su propia naturaleza de la interceptación de las comunicaciones, la cual y en principio, no es deseable ni lícita en una sociedad democrática. El Tribunal no acepta, sin embargo, que la utilización de los datos así obtenidos no pueda plantear problemas en relación con el artículo 8. En los registros así efectuados, se contienen informaciones -en especial, los números marcados- que son parte de las comunicaciones telefónicas. En opinión del Tribunal, ponerlos en conocimiento de la Policía, sin el consentimiento del abonado, se opone también al derecho confirmado por el artículo 8" (apartado 84).

La afirmación de que los números de teléfono marcados, la hora y la duración de la llamada, forman parte de los datos externos al proceso de comunicación, pero requieren el mismo nivel de protección que el contenido de aquélla, siendo decisiva, sólo resuelve

una pequeña parte del problema. Hoy en día la telefonía móvil genera toda una serie de datos de tráfico que van mucho más allá de aquéllos respecto de los que el TEDH tuvo ocasión de pronunciarse, hace ahora más de 23 años.

La Directiva 97/66/ CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al Tratamiento de Datos Personales y Protección de la Intimidad en el sector de las Telecomunicaciones, incorporó en su Anexo una enumeración de los datos de tráfico definidos con carácter general en el art. 6.2. Allí podía leerse: "...a los efectos a que se hace mención en el apartado 2 del artículo 6, podrán procesarse los siguientes datos que incluyan: el número o la identificación de la estación del abonado, la dirección del abonado y el tipo de estación, el número total de unidades que deben facturarse durante el ejercicio contable, el número del abonado que recibe la llamada, el tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitido, la fecha de la llamada o del servicio, otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes".

La simple lectura de esa enumeración ya anticipa la necesidad de operar con un criterio selectivo que, en atención a la funcionalidad del dato, permita discernir si su incorporación al proceso penal ha de realizarse, siempre y en todo caso, conforme a las normas que tutelan y protegen el secreto de las comunicaciones.

La mencionada Directiva 97/66/CE fue expresamente derogada por la Directiva 2002/58 /CE, del Parlamento Europeo, relativa al Tratamiento de los Datos Personales y Protección de la Intimidad en el Sector de las Comunicaciones electrónicas. En su art. 2.b) ofrece una definición auténtica de dato de tráfico entendiendo por tal "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma". Esa definición se reitera en su instrumento de transposición, concretamente, en el Real Decreto 424/2005, 15 de abril, por el que se aprobó el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (art. 64 a).

Pero además de la categoría de datos de tráfico, la indicada Directiva acoge un tratamiento singularizado para lo que denomina los «datos de localización», definiendo éstos como "...cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público" (art. 2.c). También incluye entre las definiciones legales la referida al «servicio con valor añadido», esto es, "todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación" (art. 2.g).

Cuanto antecede advierte que el concepto de datos externos manejado por el TEDH en la tantas veces invocada sentencia del Caso Malone, ha sido absolutamente desbordado por una noción más amplia, definida por la locución "datos de tráfico", en cuyo ámbito se incluyen elementos de una naturaleza y funcionalidad bien heterogénea. Y todo apunta a que la mecánica importación del régimen jurídico de aquellos datos a estos otros, puede conducir a un verdadero desenfoque del problema, incluyendo en el ámbito de la protección constitucional del derecho al secreto de las comunicaciones datos que merecen un tratamiento jurídico diferenciado, en la medida en que formarían parte, en su caso, del derecho a la protección de datos o, con la terminología de algún sector doctrinal, del derecho a la autodeterminación informativa (art. 18.4 CE).

C) Conforme a esta idea, **la Sala no puede aceptar que la captura del IMSI por los agentes de la Guardia Civil haya implicado, sin más, como pretende el recurrente, una vulneración del derecho al secreto de las comunicaciones.** No es objeto del presente recurso discernir, entre todos los datos de tráfico generados en el transcurso de una comunicación telefónica, cuáles de aquéllos merecen la protección reforzada que se dispensa en el art. 18.3 de la CE. En principio, ese carácter habría de predicarse, actualizando la pauta interpretativa ofrecida por el TEDH, de los datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Y la información albergada en la serie IMSI, desde luego, no participa de ninguna de esas características. Varias razonas avalan esta idea.

En primer lugar, que en los supuestos de telefonía móvil con tarjeta prepago esa información, por sí sola, no permite obtener la identidad de los comunicantes, la titularidad del teléfono móvil o cualesquiera otras circunstancias que lleven a conocer aspectos susceptibles de protección por la vía del derecho al secreto de las comunicaciones. En segundo lugar, que esa numeración puede llegar a aprehenderse, incluso, sin necesidad de que el proceso de comunicación se halle en curso. Con ello quiebran también las ideas de funcionalidad y accesoriedad, de importancia decisiva a la hora de calificar jurídicamente el alcance de la tutela constitucional de esa información.

D) **Es evidente, sin embargo, que la negación del carácter de dato integrable en el contenido del derecho al secreto de las comunicaciones, no implica su irrelevancia constitucional**. La información incorporada a la numeración IMSI es, sin duda alguna, un dato, en los términos de la legislación llamada a proteger la intimidad de los ciudadanos frente a la utilización de la informática (art. 18.4 de la CE). Y es que, por más que esa clave alfanumérica, por sí sola, no revele sino una sucesión de números que ha de ser completada con otros datos en poder del operador de telefonía, su tratamiento automatizado haría posible un significativo nivel de injerencia en la privacidad del interesado. Que la numeración del IMSI encierra un dato de carácter personal es conclusión que se obtiene por la lectura del art. 3.a) de la LO 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal, con arreglo al cual, dato personal es "...cualquier información concerniente a personas físicas identificadas o identificables".

Admitido que esa numeración IMSI es integrable en el concepto de dato personal, por cuanto que mediante su tratamiento automatizado y su interrelación con otros datos en poder del operador puede llegar a obtenerse, entre otros datos, la identidad del comunicante, obligado resulta precisar el régimen jurídico de su cesión y, sobre todo, el de su aprehensión mediante acceso.

No faltan preceptos en nuestro sistema que deberían ofrecer, al menos en el plano formal, una respuesta a nuestro interrogante. Así, el art. 11.2.1 de la LO 15/1999, 13 de diciembre, sobre Protección de Datos de Carácter Personal, al ocuparse de la comunicación de los datos personales establece como principio de carácter general que "...los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Sin embargo, la propia Ley excluye la necesidad de ese consentimiento "...cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la

comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas" (art. 11.2.d).

Con similar inspiración, el art. 12.3 de la Ley 34/2002, 11 de julio, de Servicio de la Sociedad de la Información y del Comercio Electrónico, establecía en su art. 12.3 que "...los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguarda de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales". Este precepto ha sido derogado por la Ley 25/2007, 28 de octubre, a la que luego nos referiremos, habiéndose añadido un art. 12 bis por la Ley 56/2007, 28 de diciembre, sobre Medidas de Impulso de la Sociedad de la Información.

Una aproximación hermenéutica basada en la simple literalidad de aquellos preceptos, podría llevar a enunciar que, en los casos a que se refiere el art. 12.3, la cesión de datos personales no está sujeta a reserva jurisdiccional. De hecho, así lo ha entendido en más de una ocasión la Agencia de Protección de Datos, órgano público de carácter autónomo que, conforme al art. 37.1.a) de la LO 15/1999, 13 de diciembre, tiene por misión "...velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos" (cfr. informes 135/2003 y 297/2005).

Esta primera afirmación, sin embargo, no puede aceptarse sin más. En principio, ya hemos apuntado supra cómo de acuerdo con el estado actual de la jurisprudencia constitucional, todos aquellos datos que puedan considerarse integrados en el secreto de las comunicaciones, se sustraen al régimen de tutela constitucional que ofrece el art. 18.4 de la CE y sus leyes de desarrollo, acogiéndose a la protección reforzada que impone el art. 18.3 en el que, siempre y en todo caso, se exige autorización judicial para cualquier forma de injerencia en el secreto de las comunicaciones. Así lo entendió, por otra parte, la Consulta de la Fiscalía General del Estado 1/1999, 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones. En ella se razonaba que el art. 11.2.d) de la LO 15/1999, 13 de diciembre, en cuanto autoriza un flujo inconsentido de información hacia autoridades no judiciales debe ser interpretado con extraordinaria cautela cuando el dato cuya cesión se pide está protegido ab origine por una garantía constitucional autónoma, como el secreto de las comunicaciones -art. 18.3 CE-, porque si bien el sacrificio del derecho fundamental configurado a partir del art. 18.4 de la CE como derecho a controlar el flujo de las informaciones que conciernan a cada persona - STC 11/1998, 13 de enero, F. 5º - puede ser justo y adecuado cuando dicha información no sea particularmente sensible, el sacrificio de otros derechos fundamentales concurrentes exigirá una previsión legal más específica y concreta - STC 207/1996, F. 6.A- que la que dispensa la cláusula abierta enunciada en el art. 11.2.d).

E) Sea como fuere, **la entrada en vigor de la Ley 25/2007, 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones -dictada para la transposición de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo-, obliga a un replanteamiento de buena parte de las posiciones doctrinales e institucionales que habían relativizado, en determinados casos, la exigencia de autorización judicial para la cesión de tales datos.**

En principio, no deja de llamar la atención la clamorosa insuficiencia, desde el punto de vista de su jerarquía normativa, de una Ley que, regulando aspectos intrínsecamente ligados al derecho al secreto de las comunicaciones, y a la protección de datos personales, no acata lo previsto en el art. 81.1 de la CE. Pese a todo, la Exposición de Motivos de la citada Ley 25/2007 proclama que "...la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, esencialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afectan a una comunicación o comunicaciones concretas, exigirá siempre autorización judicial previa".

El legislador español ha optado, así lo afirma de manera expresa, por un sistema de autorización judicial. El art. 1 de la Ley 25/2007 señala que es su objeto "...la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales". El art. 6.1 de la misma Ley establece con toda claridad que "los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial". Y entre los datos que han de ser objeto de conservación por los operadores se incluye, además de otros minuciosamente señalados en aquella ley, "la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada (...) y de la parte que recibe la llamada" (art. 3.1.e.2.ii e iv).

Tampoco ahora la aparente claridad de ese precepto resuelve satisfactoriamente el interrogante suscitado en el presente recurso. Se oponen a ello dos razones básicas. La primera, la llamativa regulación de un sistema específico y propio para los servicios de telefonía mediante tarjetas de prepago (disposición adicional única de la Ley 25/2007); la segunda, la ausencia de un régimen particularizado para aquellos casos, no de cesión del dato representado por la tarjeta IMSI, sino de acceso a ese mismo dato al margen de la entidad responsable de los ficheros automatizados.

F) Respecto de la primera de las cuestiones, la lectura de la disposición adicional única de la tantas veces citada Ley 25/2007 sugiere la clara voluntad legislativa de fijar un régimen particularizado para la telefonía celular mediante tarjeta prepago. Su análisis encierra una especial importancia para el supuesto que nos ocupa, toda vez que las comunicaciones del recurrente con otros miembros de la organización se verificaban mediante telefonía móvil en su modalidad de prepago.

El apartado 1 de la mencionada disposición establece la obligación de los operadores de llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta con dicha modalidad de pago. En el mismo apartado se precisan los aspectos formales de esa identificación que, tratándose de personas físicas, consistirá en "...el documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento".

Pues bien, el apartado 2 de la mencionada disposición adicional única, aclara que "...desde la activación de la tarjeta de prepago (...) los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera". Y con visible redundancia, el apartado 4 repite el mismo mensaje para aquellos casos en los que tales datos de identificación "...les sean requeridos (...) con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales".

Podría pensarse que este precepto, más allá del deseo estatal de someter a mayor control la telefonía móvil en su modalidad prepago, no añade nada al régimen general de autorización judicial establecido por el art. 6.1 de la Ley 25/2007. Sin embargo, la mención individualizada a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, funcionarios de Vigilancia Aduanera y personal del Centro Nacional de Inteligencia, cuando actúan en el ejercicio de las funciones de investigación y detección de los delitos, frente a los agentes facultados -esos mismos agentes cuando actúan con el respaldo de una autorización judicial previa- parecería avalar la idea de una excepción al régimen general.

No es fácil aceptar este criterio. De una parte, porque esta misma Sala ha dicho -y hemos transcrito supra- que el formato tecnológico en el que el proceso de comunicación se verifica no debe implicar una disminución del canon constitucional de protección del derecho al secreto de las comunicaciones. Además, carecería de sentido que la Ley 25/2007 se propusiera regular un singularizado régimen de injerencia en la telefonía mediante tarjeta prepago cuando uno de los elementos definitorios de esa modalidad de comunicación, esto es, la posibilidad de asumir la condición de usuario sin revelar datos de identificación personal, está destinada a su desaparición, según se desprende de los apartados 7 y 8 de la mencionada disposición adicional única.

G.- Aceptado, pues, que **nuestro régimen jurídico impone la exigencia de autorización judicial para la cesión por las operadoras del IMSI -también en los casos de telefonía móvil mediante tarjeta prepago-, hemos de cuestionarnos si el acceso a ese dato -no su cesión- puede obtenerse legítimamente por las Fuerzas y Cuerpos de Seguridad del Estado, sin necesidad de autorización judicial previa.**

La primera idea que sugiere la lectura de la Ley 25/2007 es que sus preceptos se centran en ofrecer un casuístico régimen jurídico de la conservación y cesión por las operadoras de los datos relativos a las comunicaciones electrónicas -en nuestro caso, del IMSI-, pero no aborda la regulación de su recogida por las Fuerzas y Cuerpos de Seguridad del Estado, no desde los ficheros automatizados que obran en poder de los prestadores de servicio, sino desde el propio teléfono celular. Cobra todo su significado el régimen jurídico del acceso a los ficheros contemplado por la LO 15/1999, 13 de diciembre, de protección de datos. Y es que frente al silencio de la nueva regulación, esta Ley dispone que "**la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en**

ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (art. 22.2). Además, "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" (art. 22.3).

Esa capacidad de recogida de datos que la LO 15/1999, 13 de diciembre, otorga a las Fuerzas y Cuerpos de Seguridad del Estado, no puede, desde luego, servir de excusa para la creación de un régimen incontrolado de excepcionalidad a su favor. Pero tampoco cabe desconocer que la recogida de ese dato en el marco de una investigación criminal -nunca con carácter puramente exploratorio-, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional. También parece evidente que esa legitimidad que la Ley confiere a las Fuerzas y Cuerpos de Seguridad del Estado nunca debería operar en relación con datos referidos al contenido del derecho al secreto de las comunicaciones (art. 18.3 de la CE) o respecto de datos susceptibles de protección por la vía del art. 18.4 de la CE que afectaran a lo que ha venido en llamarse el núcleo duro de la privacidad o, con la terminología legal, los datos especialmente protegidos (art. 7.2 LO 15/1999).

Hecha la anterior precisión, está fuera de dudas que el IMSI, por sí solo, no es susceptible de ser incluido en alguna de esas dos categorías. Ni es un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos. Como ya se razonó supra, ese número de identificación sólo expresa una serie alfanumérica incapaz de identificar, por su simple lectura, el número comercial del abonado u otros datos de interés para la identificación de la llamada. 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.

Y esto fue sencillamente lo que ocurrió en el presente caso. Según puede leerse en el F. 1º B, "...la concordancia de estas claves numéricas tras varias vigilancias sobre las mismas personas les permitió informar al Juzgado de los números IMSI utilizados por los sospechosos, solicitando autorización para recabar el número de teléfono comercial asociado y su observación (...). Para la obtención del número de teléfono a través de las compañías operadoras, en este caso, la Guardia Civil ya recabó la autorización judicial". Así se desprende, además, de la lectura de los folios 51 y ss, en los que se contiene la

primera solicitud de la fuerza actuante y del folio 60, en el que se recoge el auto dictado por el Juez de instrucción, previo informe favorable del Ministerio Fiscal.

No es equiparable el supuesto ahora enjuiciado al que fue objeto de solución por la STS 130/2007, 19 de febrero. En esta última resolución -que acoge dos votos particulares que concluyen la innecesariedad de autorización judicial por una vía argumental distinta a la aquí defendida-, puede leerse: "...**la policía, antes de acudir al juzgado en demanda de una autorización para intervenir los teléfonos de referencia, habría procedido por sus propios medios técnicos a injerirse en el curso de algunas comunicaciones telefónicas, consiguiendo así los números de los correspondientes a un determinado usuario**. Es lo que resulta del oficio que abre la causa en relación con la afirmación testifical antes transcrita, en la que el funcionario declarante precisó que el ingenio técnico utilizado permite la detección de «los números de teléfono que se están utilizando»" (F. 1º). El hecho añadido de que alguno de los agentes que declararon en el juicio oral se amparara en el secreto profesional para negar toda explicación respecto del modo en que aquel número fue obtenido, añadió entonces una sombra de duda acerca de que el cruzamiento de datos que hizo posible el acceso al número telefónico se hubiera obtenido sin las debidas garantías.

Tampoco es identificable con el supuesto de hecho valorado por la sentencia de esta misma Sala núm. 23/2007, 23 de enero. En este caso, **la intervención de la serie numérica IMEI -no la IMSI- se logró a partir de tres aparatos de telefonía móvil que habían sido sustraídos a la víctima de un delito de robo**. Y, lo que es más relevante, esta resolución fue dictada cuando todavía no había sido aprobada la Ley 25/2007, 18 de octubre que, como hemos tenido ocasión de razonar supra, impone la autorización judicial para la cesión de datos por los operadores de telefonía.

En el supuesto que motiva el presente recurso, pues, ninguna vulneración del derecho al secreto de las comunicaciones se produjo. De ahí la necesidad de desestimar el motivo por su falta de fundamento (art. 885.1 LECrim).

[…]

III. FALLO

Que debemos declarar y declaramos no haber lugar a los recursos de casación promovidos por las respectivas representaciones legales de Adolfo, Blas, Daniel Eusebio, Marí Jose y Gonzalo. Asimismo, declaramos haber lugar al recurso de casación formulado por la representación legal de Arturo, por estimación parcial de su segundo motivo, por infracción de ley, interpuesto contra la sentencia de fecha 27 de junio de 2007, dictada por la Sección Primera de la Audiencia Nacional, en causa seguida contra aquéllos por delitos contra la salud pública, falsedad en documento oficial y tenencia ilícita de armas, casando y anulando dicha resolución y procediendo a dictar segunda sentencia, con declaración de oficio de las costas procesales.

[…]