# CONFIDENCIALIDAD, SECRETO DE LAS COMUNICACIONES E INTIMIDAD EN EL ÁMBITO DE LOS DELITOS INFORMÁTICOS.-

**Por JOSE DIAZ CAPPA**

**FISCAL DE LA FISCALÍA SUPERIOR DE ILLES BALEARS**

**DELEGADO DE CRIMINALIDAD INFORMÁTICA**

**www.josediazcappa.es**

**I) INTRODUCCIÓN. Confidencialidad. Comunicación: contenido y datos de tráfico. Comunicación: en proceso y terminada. Comunicación: enviada y recibida. II) TRATAMIENTO LEGAL DE LA CUESTION. Referencias internacionales. Secreto de las comunicaciones e intimidad personal. III) ANALISIS DE LA JURISPRUDENCIA APLICADA Y APLICABLE. IV) CONSIDERACIONES FINALES. CONCLUSIONES. LA STS DE 18 DE MARZO DE 2010.**

***Sinopsis:*** **El presente artículo tiene por objeto argumentar, a propósito de la STS nº 247/2010, Sala 2ª, de 18 de marzo de 2010[1], y de la STC nº 123/2002, de 20 de mayo[2], entre otras referencias, la posibilidad de no necesidad de previa autorización judicial, -que ahora se exige inexcusablemente-, para la cesión de los datos generados o tratados conforme a lo dispuesto en el actual art. 1[3] de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.**

***Resumen:*** **La ineludible adecuación a la Constitución de las diligencias de investigación e instrucción practicadas en los procesos penales, plantea, en relación con la llamada *criminalidad informática,* nuevas vías de posible interpretación. La novedad y especial idiosincrasia de este tipo de delincuencia que, en la mayoría de las ocasiones, hace imprescindible para su persecución la afectación de derechos fundamentales, y especialmente los relativos al secreto de las comunicaciones y a la intimidad personal, así como la innegable relación -y no en pocas veces confusión simbiótica- con el ámbito relativo a la protección de los datos personales durante la**

[1] Tribunal Supremo, Sala Segunda, de lo Penal, Ponente Excmo. Sr. José Ramón Soriano Soriano. Recurso nº 121/2009. STS Nº 247/2010.

[2] Tribunal Constitucional, Sala Primera, Sentencia Nº 104/2006, de 3 Abril de 2006. Recurso nº 7224/2002. Ponente: Excma. Sra. Casas Baamonde, María Emilia. Nº de Sentencia: 104/2006.

[3] Dice el art. 1.1. que *"Esta Ley tiene por 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".*

**instrucción de los procesos penales, así como la proliferación de normativa internacional en la materia posteriormente trasladada al ámbito nacional, permiten nuevas reflexiones sobre las formas de acceder a tales derechos fundamentales. En este artículo el autor se plantea y argumenta, poniendo especialmente el énfasis en la nota común de confidencialidad que a todos los derechos fundamentales citados atañe, y haciéndose eco de normativa nacional e internacional y de jurisprudencia al respecto, la no necesidad de contar siempre con autorización judicial *ex ante* habilitante para ciertas injerencias en aquellos derechos, y de ponderar las opciones legales de investigación por parte del Ministerio Fiscal y de la Policía Judicial dando mayores dosis de relevancia, en pro también de la seguridad jurídica y sin obviar nunca el necesario control judicial, a los criterios de anulabilidad sobre los de nulidad radical y absoluta.**

## I.- INTRODUCCION.- Confidencialidad. Comunicación: contenido y datos de tráfico. Comunicación: en proceso y terminada. Comunicación: enviada y recibida.

El aumento, sin duda significativo y en constante progreso, de la denominada ciberdelincuencia, -o delincuencia (o criminalidad) informática-[4], arrastra ya, en relativamente poco tiempo, un importante hándicap, repercutible sobre todo en el campo procesal, y que, en mi opinión, puede obedecer a un exceso de celo garantista desde el punto de vista legal apoyado en una cierta disparidad de corrientes jurisprudenciales. Me refiero a la **interpretación del término "confidencialidad", y en concreto, a la incidencia de dicho concepto en las posibilidades de investigación criminal de este tipo de delincuencia**, que, más allá de la simple relación con el mundo de las comunicaciones electrónicas, con las TIC[5] y la Sociedad de la Información, puede hacer referencia en un momento dado a cualquier modalidad delictiva. En unos casos, porque la propia investigación en el ámbito informático es necesaria para la resolución de la infracción penal por su propia *"naturaleza informática"* (pensemos en la estafas a través de la Red, en los tipos penales de descubrimiento y revelación de secretos, en los delitos de daños informáticos, pornografía infantil, *child grooming*, delitos contra la libertad, contra el honor, secretos empresariales, etc.), pero también, porque cualquier tipo de infracción penal puede tener como base o parte de su posible acreditación, un elemento probatorio informático: así, un e-mail enviado, el contenido de un SMS, el estudio de una red social en que el posible delincuente haya dejado indicios de su eventual participación delictiva, una dirección IP comprometedora, o un estudio pormenorizado de cualquier ordenador o hardware…, pueden servir o ser esenciales como prueba, informáticamente obtenida, de la participación en un hecho criminal. Pocos actos investigadores de delitos importantes y con cierta entidad dejan al margen, hoy día, un estudio o repaso, siquiera sea rápido, de las opciones investigadoras que ofrece la Sociedad de la Información.

[4] Sin duda, uno de los campos del Derecho Penal que, a consecuencia de su auge y constante innovación, requerirá cada vez de una mayor especialización.

[5] Definidas en Wikipedia como "las **Tecnologías de la Información y la Comunicación** (**TIC**, **TICs** o bien **NTIC** para *Nuevas Tecnologías de la Información y de la Comunicación* o **IT** para *«Information Technology»*) agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet, telecomunicaciones. (http://es.wikipedia.org/wiki/Tecnologias-de-la-información-y-comunicación)

Además, el abanico de posibilidades de formas de comunicación a través de Internet (e-mails, chats, foros, Messenger, videoconferencias…) y su carácter público o privado, hacen aún más interesante y complicada la empresa investigadora que al efecto se inicie.

Puesto que en esa labor de investigación del delito nos adentramos en el siempre resbaladizo mundo de los **derechos fundamentales**, es necesario ir desgajando algunos aspectos jurídicos para evitar que la eventual necesidad de invadir los mismos en el marco de una investigación criminal, pueda poner en peligro el éxito de la misma de hacerse de forma legal o jurisprudencialmente irregular.

Claro es que desde el punto de vista lingüístico[6] puede aparecer claro el halo de intimidad, privacidad, secreto y seguridad que tras el concepto de **confidencialidad** se deja entrever. Incluso, acercándonos un poco más al significado del término en relación con la denominada *seguridad informática*[7], no deja de perder su significado último: la consideración de secreto, en sentido amplio, de la comunicación entre las personas, y respecto de aquello que no se quiere que se conozca, y no sólo del contenido mismo de lo comunicado, -lo cual aparece como evidente-, sino incluso también, del hecho mismo de que la comunicación ha existido. Esto es, tan importante resulta para el "*hecho confidencial*" la ignorancia ajena de lo que se ha trasmitido en esa comunicación, como de aquello que pueda constatar que esa comunicación se ha producido: cuándo, cómo, dónde y entre quiénes. Por tanto, cualquier dato que permita ese conocimiento, debe participar, en sentido amplio, de la misma protección legal y judicial que la comunicación en sí misma.

Sin embargo, las innumerables y variadas formas de comunicación y la posible transmisión de todo tipo de elementos, objetos e información a través de Internet[8], **hace necesario replantearse el ajuste a Derecho y la legalidad de las diferentes opciones de investigación de los hechos ilícitos cometidos a través de las Nuevas Tecnologías de la Información y de la Comunicación.** Y no sólo Internet. Y todo ello sin minusvalorar ni poner en riesgo ninguno de los ámbitos propios de los derechos fundamentales y la protección legal de los datos personales, ni, por supuesto, la protección judicial de los mismos.

---

[6] El diccionario de la Real Academia de la Lengua Española define confidencial como *"Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas".*

[7] Nos dice la Wikipedia (http://es.wikipedia.org/wiki/Confidencialidad) que la confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado: de hecho, un asunto de gran interés es el problema de garantizar la confidencialidad de la comunicación utilizada cuando el sistema es inherentemente insegura (como Internet).

[8] O como dice la Exposición de Motivos de la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, *"La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también* ***datos*** *en soportes y formatos diversos".*

Ahora bien, cuando, al margen de la pura semántica, nos tenemos que acercar al **concepto de confidencialidad desde el punto de vista legal y jurisprudencial,** existe, en la actualidad y en mi opinión, una cierta dosis de falta de concreción. Me explico, e intentaré hacerlo en estas breves líneas partiendo del contenido del artículo 18 de la CE[9] en el que se otorga protección constitucional a varios derechos fundamentales. Además de la referencia a la inviolabilidad del domicilio, -sin duda también trascendente, y mucho, en materia de delincuencia informática, pero que exige su estudio en otro ámbito diferente al tema que aquí abordamos-, se encuentran recogidos otros dos en concreto: **la intimidad personal (18.1) y el secreto de las comunicaciones (18.3)**. Y, además, la referencia protectora constitucional definida en el art. 18.4 como **limitación legal al uso de la informática** para garantizar, entre otras cosas, la intimidad personal y familiar.

Así pues, **trataré de argumentar que para la investigación criminal de un hecho delictivo, dentro del abanico de los denominados delitos informáticos** (aunque perfectamente extrapolable a otro tipo de delincuencia), **no es siempre imprescindible una resolución judicial *ex ante* habilitante de la que dependa la plena validez de la intromisión en un derecho fundamental**. Para ello, hemos de tener en cuenta **varias premisas**, ahora sólo apuntadas, y que desarrollaré a lo largo del presente artículo:

a) Lo realmente esencial es la **confidencialidad. Género de una especie donde estarán comprendidos los derechos a la intimidad, secreto de la comunicación y protección de los datos personales.** Cada una de estas especies tiene una fórmula de protección legal y judicial diferente.
b) La **comunicación no es sólo el contenido de lo comunicado, sino también todos aquellos datos (de tráfico y de localización –los denominados *logs*-) que permitan identificar cualquier aspecto relativo a la comunicación en sí y a su existencia misma** (lugar, momento, comunicantes, etc.). Sin embargo, estos últimos, **los datos, no deberían estar amparados por la rigidez legal de la exigencia previa de aprobación judicial** para el acceso a los mismos por los diferentes operadores habilitados para la investigación criminal.

[9] CE *Artículo 18.1. 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 el 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.*

c) **La <u>comunicación terminada</u> o ya realizada no es igual a la <u>comunicación en proceso</u> y en progreso**, y, al igual que en el caso anterior y en lo que a los datos tangenciales a la comunicación se refiere, no deberían ser tampoco objeto de la rigidez legal de su sometimiento previo a la aprobación judicial.
d) No es lo mismo, tampoco, **<u>comunicación enviada</u>** que **<u>comunicación recibida.</u>** A efectos del tema que abordamos, lo primero es lo que marca el proceso de comunicación y sus datos, y la existencia de todo ello. Es lo esencial. Lo segundo, simplemente, supone la efectividad del envío de lo comunicado, y, además, puede suponer, el conocimiento por el receptor del contenido de lo comunicado, si bien esto último puede no haber sucedido[10].

## II.- TRATAMIENTO LEGAL DE LA CUESTION.- Referencias internacionales. Secreto de las comunicaciones e intimidad personal.-

Como expuse anteriormente, intimidad, secreto y limitación de uso de la informática respecto de los datos personales, son parte, sin duda del concepto genérico y más amplio de confidencialidad, y lo realmente importante es saber qué derecho fundamental se está realmente protegiendo en cada momento para salvaguardar la confidencialidad que a todos aquellos afecta.

La cuestión se apunta con mayor claridad haciendo un **recorrido jurídico por las normas del ordenamiento jurídico nacional e internacional** que tienen relación con la cuestión:

En primer lugar hemos de recordar que la **Ley de Enjuiciamiento Criminal sólo hace reserva de autorización judicial[11] cuando se trate de respetar el derecho**

[10] En la Ley 25/2007, 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, extiende la obligación de conservación a las llamadas infructuosas, no así a las no conectadas. En concreto dispone que: *"2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada. 3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados."*

[11] **Artículo 579**
**1.** Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

**al secreto de las comunicaciones, pero no cuando se trate del derecho a la intimidad**, y, por supuesto, tampoco en los casos en que la incidencia de la vulneración puede no ser sino meramente civil o administrativa[12]. Lo veremos más adelante como criterio jurisprudencial ya acuñado.

Por otro lado, la **Ley 25/2007 de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones**[13] dispone, en su artículo 1 lo siguiente: *"Esta Ley tiene por 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[14] contemplados en el Código Penal o en las leyes penales especiales".*

Por lo tanto, inicialmente, necesaria autorización judicial para disponer de dichos datos. Y, ¿cuáles son esos datos? El mismo precepto nos dice, en el párrafo siguiente, que *"Esta Ley se aplicará a los* ***datos de tráfico y de localización sobre***

---

**2.** Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
**3.** De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.
**4.** En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación.

[12] Recordemos en este sentido las novedades introducidas por la Disposición Cuadragésima Tercera de la Ley 2/2011 de 4 de marzo, de Economía Sostenible (modificada a su vez por LO 4/2011, de 11 de marzo) en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual y en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, para la protección de la propiedad intelectual en el ámbito de la sociedad de la información y de comercio electrónico. Todo ello referido a otro tema, -el del apoyo judicial a un órgano administrativo para el cumplimiento de sus funciones - (en este caso la identificación del posible responsable del servicio de la sociedad de la información que estuviera realizando la conducta presuntamente vulneradora del derecho de propiedad intelectual*),* sólo tangencialmente relacionado con el que tratamos en el presente artículo.
[13] BOE nº 251, 19 de octubre de 2007.
[14] No abundaré ahora en el concepto de grave a que hace referencia este precepto, el cual, extrapolado de lo que al respecto se menciona en la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, no tiene coincidencia con la diferenciación que entre delitos graves y menos graves hace nuestro Código Penal, sino con un concepto real de gravedad en el sentido de relevancia y alarma social evidente desde el punto de vista social. Ello no deja, sin embargo, de ser una nueva marca de indefinición jurídica que, necesariamente, conlleva a una inseguridad de mismo tipo.

***personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado"***.

Se refiere pues, a los denominados en el argot informático como ***logs***, -antes mencionados-, **con exclusión expresa del contenido de las comunicaciones electrónicas**, como se advierte claramente en el párrafo tercero de éste importante precepto.

En todo ello subyace, como veremos, otro de los aspectos de especial trascendencia en el tema que nos ocupa: se trata de **elementos de identificación de una comunicación ya terminada**, (con independencia de que el receptor conozca o no su contenido) y **no en curso**. O bien en progreso pero habiendo ya generado todos los datos de tráfico necesarios. Se puede argumentar que a diferencia de las comunicaciones telefónicas, en que el momento preciso de la comunicación hace decaer al mismo tiempo la propia existencia de lo que se está comunicando, las comunicaciones electrónicas, así como los SMS o similares, pueden cursar efectivas con posterioridad al momento propio del envío, con lo que se hace difícil diferenciar de forma concreta el momento exacto de la comunicación *strictu sensu*, pero lo que es evidente es que la Ley de conservación de datos citada se refiere precisamente a eso, a datos que son susceptibles de ser conservados, que ya existen físicamente y que han tenido su proceso de producción en un momento pretérito, y, por ende, finalizados en cuanto a su posibilidad real de su obtención actual mediante la correspondiente autorización judicial. Y, no sólo eso, sino que han de servir como elementos propios de una investigación delictiva.

Este aspecto, como veremos, supone un elemento esencial en cuanto a la valoración de la necesidad o no de autorización judicial para su obtención. **Y es que, desde el momento en que el proceso de identificación del elemento comunicador, no se refiere a la comunicación en sí misma, ni a su contenido, sino a elementos tangenciales que pueden permitir la obtención de datos esenciales para la investigación, el secreto que se ampara no es ya el de la comunicación en sí, sino el de la esfera personal e íntima de los posibles intervinientes**. Así, si para la protección constitucional del derecho fundamental a la intimidad no hay reserva expresa de autorización judicial, aparece excesivo que se acometa dicho proceso garantista con posterioridad, **frustrándose así las posibilidades investigadoras de la policía judicial y del Ministerio Fiscal**[15]

Como ya veremos, la posible intervención de estos últimos sobre las vulnerabilidades del derecho a la intimidad, aparecen inicialmente amparadas legal y jurisprudencialmente a través de la salvaguarda judicial *ex post* y en examen del correcto uso de los principios de necesidad, proporcionalidad y oportunidad.

[15] La Sala General no jurisdiccional, en **Acuerdo de 23 de febrero de 2010**, indica que: ***"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 "***

El principal problema de esta nueva regulación legal es que **derogó**[16] **el artículo 12 de la ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico**. El referido precepto, que llevaba como rótulo "*Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas"* tras hacer referencia a las obligaciones de conservación de los referidos datos por parte de los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos, disponía, en su número 3 que: ***"los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces y Tribunales o del Ministerio Fiscal que así lo 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, creo, recogía con mayor rigor la verdadera esencia de los contenidos afectados por los datos de tráfico relativos a las comunicaciones. Sin dejar de dudar que todos ellos afectan a la confidencialidad, lo que realmente se podría ver afectado con la intromisión en los mismos por agentes como los cuerpos policiales o el Ministerio Fiscal, no es el secreto de la comunicación en sí mismo, sino el derecho a la intimidad, respecto del que, -como ya apunta la **STC 123/2002 de 20 de mayo**, que posteriormente también aludiremos, si bien desde el punto de vista crítico-, ***"no existe en la Constitución reserva absoluta de previa resolución judicial".***

**¿Por qué se produce, sin embargo, este cambio legal, qué, al mismo tiempo, impide el cambio de criterio jurisprudencial?**

Cómo se establece en la Exposición de Motivos de La Ley 25/2007 de 18 de Octubre, de conservación de datos, tantas veces aludida, la misma tenía como principal objeto la trasposición al ordenamiento jurídico nacional de la **Directiva 2006/24/CE del Parlamento Europeo y del Consejo,** de 15 de Marzo de 2006, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de Julio*.

En ella se inspiró pues la Ley de 2007, y, para ajustar ésta a los pronunciamientos del Tribunal Constitucional respecto al derecho al secreto de las comunicaciones dispuso la necesaria autorización judicial para la cesión de los datos relativos a la misma[17], en los términos mencionados en el artículo 1 ya citado.

[16] **Disposición Derogatoria Única de la Ley 25/2007 de 18 de octubre** de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[17] Dice la Exposición de Motivos de la referida Ley que *"En este sentido, 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, especialmente, 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*

Sin embargo, **un repaso a la referida Directiva, no nos lleva necesariamente a la consideración de los denominados datos de tráfico y de localización como elementos que, aún en el marco de la comunicación, se refieran necesariamente al derecho fundamental a su secreto, en los términos del art. 18.3 de la CE, sino que, más aún al contrario, durante la mayor parte del texto de la Directiva citada, que, recordemos, conforma el espíritu y letra de la Ley 25/2007, a lo que se está haciendo referencia es al derecho a la intimidad y a la protección de los datos personales derivados de las comunicaciones electrónicas, y no al secreto de las comunicaciones.**

Así la **Directiva 2002/58/CE**[18], de que trae causa la de 2006, se refiere precisamente al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, con referencia, asimismo, a la **Directiva 95/46/CE** relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

Del mismo modo, tampoco la Directiva 2006/24/CE viene exigiendo (quizás por ese motivo) autorización judicial para esa cesión. Así, menciona en su considerando nº 17 que *"es esencial que los Estados miembros adopten medidas legislativas para asegurar que los datos conservados de conformidad con la presente Directiva solamente se faciliten a las* ***autoridades nacionales competentes***[19] *de conformidad con la legislación nacional, respetando plenamente los derechos fundamentales de las personas"*.

## III.- ANALISIS DE LA JURISPRUDENCIA APLICADA Y APLICABLE.-

La famosa (pero no reciente, como algunos se empeñen en insistir, quizás para alargar el efecto de su contenido) **Sentencia del Tribunal Europeo de Derechos Humanos, de 2 de agosto de 1984**, en el llamado caso ***Malone***, fue, entre otras amparada por nuestro Tribunal Constitucional en la **STC 123/2002, de 20 de mayo**.

---

*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 afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa".*

[18] Modificada parcialmente por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009. (Diario Oficial de la Unión Europea 18 diciembre de 2009).

[19] En este sentido, el artículo 4 de la citada Directiva, establece que: "*Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. Cada Estado definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho Internacional Público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos*

En esta última, que, sin duda, refleja los contenidos jurisprudenciales tenidos en cuenta por el legislador, según se cita en la exposición de Motivos de la Ley 25/2007, se hace referencia, inicialmente, a que *"...doctrina ha sido reiterada recientemente en la STC 70/2002, de 3 abril. En su fundamento jurídico 9 precisamos que «el art. 18.3 CE contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas, que se declara indemne frente a cualquier interferencia no autorizada judicialmente» y que «la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, **pero finalizado el proceso en que la comunicación consiste**, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»*. Remarca pues que la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación. Asimismo afirma que *"...La separación del ámbito de protección de los derechos fundamentales a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE) efectuada en esta Sentencia se proyecta sobre el régimen de protección constitucional de ambos derechos. Pues si ex art.* ***18.3 CE la intervención de las comunicaciones requiere siempre resolución judicial, "no existe en la Constitución reserva absoluta de previa resolución judicial" respecto del derecho a la intimidad personal****. Ahora bien, también respecto del derecho a la intimidad personal hemos dicho que rige como regla general la exigencia constitucional de monopolio jurisdiccional en la limitación de derechos fundamentales, si bien hemos admitido de forma excepcional que en determinados casos y con la suficiente y precisa habilitación legal sea posible que la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas…. La legitimidad constitucional de dichas prácticas, aceptada excepcionalmente, requiere también el respeto de las exigencias dimanantes del principio de proporcionalidad, de modo que mediante la medida adoptada sea posible alcanzar el objetivo pretendido —idoneidad—; que no exista una medida menos gravosa o lesiva para la consecución del objeto propuesto —necesidad—; y que el sacrificio del derecho reporte más beneficios al interés general que desventajas o perjuicios a otros bienes o derechos atendidos la gravedad de la injerencia y las circunstancias personales de quien la sufre —proporcionalidad estricta— (SSTC 207/1996, de 16 de diciembre, FJ 3; y 70/2002, de 3 de abril, FJ 10)".*

En esta dinámica, la línea argumental seguida, parecía dirigida a la constatación no sólo de la clara separación de la distinta dinámica de protección entre los dos derechos fundamentales, (secreto de las comunicaciones e intimidad) sino que, además, que el *tema decidenci* de la referida sentencia, (la legalidad de la obtención policial sin autorización judicial motivada[20]de los listados de las compañías telefónicas) debería haber sido en sentido favorable a lo así actuado policialmente, sobre todo, cuando posteriormente se pone de manifiesto en la misma sentencia que **"** *...la vulneración del derecho al secreto de las comunicaciones telefónicas requiere* ***la interferencia directa en el proceso de comunicación*** *(mutatis mutandi respecto de las comunicaciones postales STC 70/2002) mediante el empleo de cualquier artificio técnico de captación,*

[20] Pues en realidad la intervención judicial sí había existido, pero en forma de Providencia, y no de Auto.

*sintonización o desvío y recepción de la señal telefónica como forma de acceso a los datos confidenciales de la comunicación: su existencia, contenido y las circunstancias externas* del proceso de comunicación antes mencionadas. De modo que la difusión sin consentimiento *de los titulares del teléfono o sin autorización judicial de los datos de esta forma captados supone la vulneración del derecho al secreto de las comunicaciones.*

Esto es, se viene a confirmar que, para que el derecho fundamental al secreto de las comunicaciones, deba y, por tanto, los datos de tráfico que al mismo afecten deban a su vez ser considerados como tales y sometidos a la exigencia de previo control judicial, ha de tratarse de una comunicación **en proceso**[21]**.**

Es difícil, aunque podría haberlos, encontrar supuestos de petición de autorización judicial de acceso a los datos conservados conforme a la Ley 25/2007, que no formen parte ya del pasado, siquiera sea inmediato, del acto de comunicación. Y, por otro, lado, para la obtención de comunicaciones en proceso, no es necesario argumentar la necesidad de autorización judicial, la cual, evidentemente, enjugará también los datos de tráfico y localización consecuentes a la misma, para cuya obtención no será necesaria una habilitación judicial extra.

A partir de ahí, insisto, y conforme a los propios criterios jurisprudenciales que, en principio, llegan a la solución contraria, **los referidos datos conservados forman parte del derecho fundamental a la intimidad, y, como antes se apuntó, el propio Tribunal Constitucional admite la posibilidad de su solicitud policial (y creo, de forma más evidente aún, del Ministerio Fiscal) cumplidos los requisitos de idoneidad, proporcionalidad, necesidad y control judicial *ex post* mediante la ponderación del correspondiente juicio de anulabilidad.**

Añade esta sentencia (y con ello nos vamos acercando aún más al epicentro de la cuestión) que *"...es de señalar aquí que el **fundamento** del carácter autónomo y separado del reconocimiento de este derecho fundamental y de su específica protección*

[21] El propio Tribunal Constitucional, en la referida sentencia, y a modo de conclusión, dice que *"La aplicación de la doctrina expuesta conduce a concluir que la entrega de los listados por las compañías telefónicas a la policía sin consentimiento del titular del teléfono requiere resolución judicial, pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art.18.3 CE. En efecto, los listados telefónicos incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y a su duración, para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar, con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso a efectos, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión. Dichos datos configuran el proceso de comunicación en su vertiente externa y son confidenciales, es decir, reservados del conocimiento público y general, además de pertenecientes a la propia esfera privada de los comunicantes. El destino, el momento y la duración de una comunicación telefónica, o de una comunicación a la que se accede mediante las señales telefónicas, constituyen datos que configuran externamente un hecho que, además de carácter privado, puede asimismo poseer un carácter íntimo".*

*constitucional reside en* ***la especial vulnerabilidad de la confidencialidad*** *de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación. A través de la protección del proceso de comunicación se garantiza, a su vez, el carácter reservado de lo comunicado sin levantar su secreto, de forma que* ***es objeto de este derecho la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado"*** y que *"proyectando estas consideraciones sobre el derecho al secreto de las comunicaciones telefónicas, este derecho 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".*

## IV.- CONSIDERACIONES FINALES. CONCLUSIONES. LA STS DE 18 DE MARZO DE 2010.-

Conforme pues, a las mismas premisas emanadas del Tribunal Constitucional (y como veremos también, en la reciente Jurisprudencia del TS) y que terminaron con la obligación de autorización judicial previa para el acceso a los datos conservados conforme a lo dispuesto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**, se puede llegar a la conclusión contraria: la no necesidad de dicha autorización judicial para que el Ministerio Fiscal y la Policía Judicial, en su función legal y constitucional de investigación de los delitos, pueda solicitar a los diferentes operadores, los referidos datos**[22]:

Así, y a modo de **conclusiones**:

1.- Es cierto, y en ello hemos insistido, que la clave de todo es el término **CONFIDENCIALIDAD**. Dicho término es la base y el género en el que se apoyan las

[22] La línea seguida hasta ahora, o, más bien, desde la referida Ley de 2007, pues vimos la existencia de opciones legales anteriores a la misma, entiendo, apunta a un cierto desfase con la realidad actual, y además, complica, innecesariamente, la labor de investigación tanto de la policía como del Ministerio Fiscal, (más aún en un período en que la atribución de la instrucción criminal al Ministerio Fiscal va adquiriendo, cada vez, caracteres de mayor realidad).

diferentes especies a modo de derechos fundamentales, y, en concreto, el secreto de las comunicaciones y la intimidad. Ambos tienen, como clave, el carácter reservado y privado de la evitación ajena del conocimiento de lo íntimo, de lo confidencial. Ya hemos visto como el propio TC en la sentencia mencionada y en las que también menciona en la misma, reconoce la existencia de una ***"confidencialidad de la comunicación"*** y una ***"confidencialidad de las circunstancias o datos externos de la conexión"*** cada una de las cuales repercute en un derecho fundamental distinto: el secreto de la comunicación, en el primer caso, y el derecho fundamental a la intimidad personal, en el segundo. Ello debe traducirse en una necesidad de protección procesal y constitucional también diferente.

2.- Que, como hemos ido argumentando, cada uno de esos derechos dispone de un mecanismo procesal protector diferente, **apareciendo como obligatoria la autorización judicial previa para la intervención de las comunicaciones, y no existiendo tal reserva constitucional, respecto del derecho a la intimidad.**

3.- Que, efectivamente, la **comunicación, o comunicaciones,** en general, conllevan una serie de **datos connaturales a la misma, que merecen la misma protección que el hecho mismo del contenido de la comunicación**. Ahora bien, dichos datos de tráfico y de localización, **merecen el mismo trato procesal, legal y constitucional que el derecho fundamental del que traen causa**. Si lo es el secreto de las comunicaciones, la autorización judicial previa; si lo es del derecho a la intimidad, el control judicial no necesariamente ex ante.

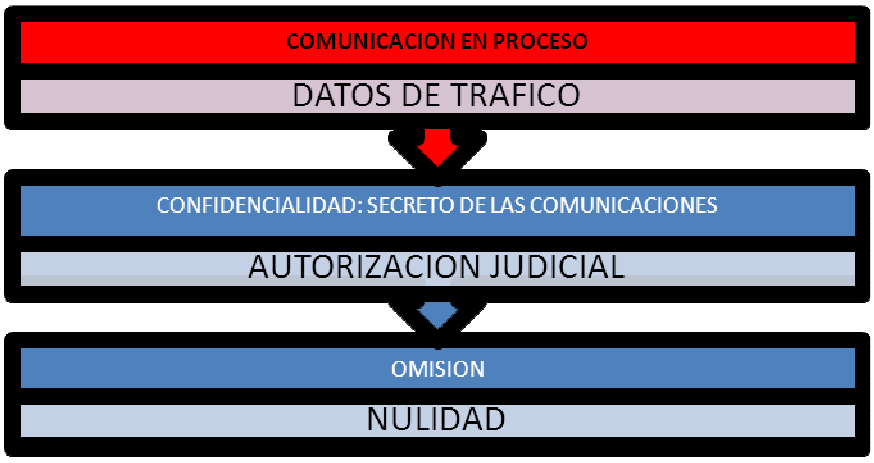
4.- Que para poder realizar la referida discriminación, aparece como esencial distinguir entre **que la comunicación esté o no en proceso.** Si lo está, dicha comunicación precisará de autorización judicial para su conocimiento por otros operadores, pues es la confidencialidad propia del proceso comunicativo en marcha lo que está en juego, y, junto con su contenido, los datos de tráfico y localización anexos, dependientes e inseparables del mismo. Pero, si el proceso comunicador ya no está en proceso, con independencia del conocimiento efectivo de su contenido por el receptor, lo que está en juego entonces es la confidencialidad propia del derecho a la intimidad, y, por ende, los datos conexos a esa comunicación terminada, esos datos que son susceptibles de ser conservados y que se mencionan en la Ley de 2007, ya existen físicamente y ya han tenido su proceso de producción en un momento pretérito, y, por ende, finalizados en cuanto a su posibilidad real de su obtención actual mediante la correspondiente autorización judicial. **Su acceso posterior por otros operadores y autoridades legalmente determinados, sería posible pues sin necesidad de la autorización judicial recogida con carácter obligatorio en el artículo 1 de su texto**. Y ello, además, sin necesidad de acudir a jurisprudencia distinta de la que, aparentemente, plantea una única solución, y, además, radicalmente contraria a la que se propugna en este artículo.

5.- Por tanto, sin mermar en absoluto la consideración de fundamentales de los derechos a los que venimos refiriéndonos, lo cierto que, como sabemos y hemos

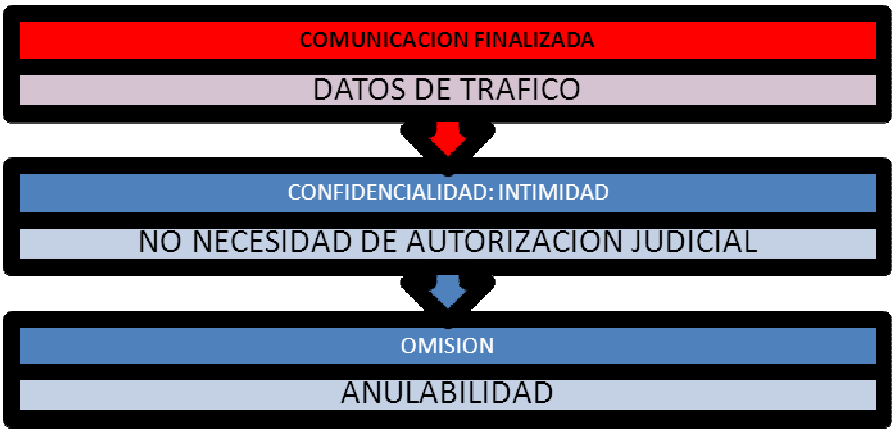
comentado, las limitaciones a los derechos contenidos en el art. 18.1 (intimidad) y 18.4 (límites al uso de la informática) no están sometidos a la necesaria habilitación judicial como sí lo está el secreto a las comunicaciones del art. 18.3. y ello supone que, **ciertas partes tangenciales a la comunicación, pero que no formen ya parte real de la misma porque la referida comunicación ya esté finalizada, deberían, sin dejar de ser confidenciales, considerarse como parte de la intimidad de la esfera personal, la cual podría ser objeto de consideración a efectos de investigación e instrucción por parte de la policía y del Ministerio Fiscal con la oportuna habilitación legal y con respeto a los debidos parámetros de proporcionalidad, idoneidad y beneficio para el interés público.**

Esto es, debemos dar **un paso más**, **desde la nulidad radical** por falta de habilitación judicial, **a la posibilidad de anulabilidad** de lo actuado por el Ministerio Fiscal y la Policía Judicial, que permitiría el necesario **control judicial** del proceso de enjuiciamiento de las infracciones penales y de la validez de los métodos de investigación usados.

**ESQUEMÁTICAMENTE VENDRIA A SER LO SIGUIENTE:**




---




Me quedo, por tanto, con los **nuevos aíres jurisprudenciales** que se apuntan en la **STS 18 de marzo de 2010, citada al inicio de este trabajo y que, a modo de colofón quiero reseñar en estas líneas. Nos dice la referida Sentencia, cuya lectura completa se antoja necesaria[23], que:**

*"La correcta interpretación de esta doctrina* (se refiere a la contenida en la STDH de 1984 *ut supra* citada) *nos debe llevar a la distinción de cuándo unos datos personales pueden afectar al secreto a las comunicaciones y cuándo conservados y tratados por las Operadoras, no se están refiriendo a comunicación alguna, es decir, datos estáticamente almacenados, conservados y tratados por operadores 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:*

*b) datos o circunstancias personales referentes a la intimidad de una persona (art. 18-1º C.E.), 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. 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.".***

Esta sentencia, si bien se define en relación con la normativa procesal aplicable al momento que correspondía al enjuiciamiento de los hechos, (anteriores a la Ley 25/2007) no deja de contrastar aquellos con la nueva regulación, y, en base a aquella,

[23] En especial los Fundamentos Jurídicos segundo a quinto, ambos inclusive.

deja entrever, entiendo, una cierta actual rigidez legal en la nueva exigencia general de autorización judicial previa para la cesión de los datos, y avala ampliamente la licitud[24] de la actuación llevada a cabo por el Ministerio Fiscal[25] en la investigación al solicitar determinados datos[26] contrastando ello con disposiciones legales, aún actuales, y de mayor rango normativo, como la LO 15/1999 de 13 de diciembre, de Protección de Datos Personales o *"...el art. 11.2 d) de la Ley Orgánica 15/1999 de 13 de diciembre nos dice que el consentimiento del interesado a que se refiere el párrafo anterior no será necesario.... d) "Cuando la comunicación que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal , los Jueces o Tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tienen atribuidas". Por su parte la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones, cuyo articulado se remite al art. 12 de la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (ahora derogada por la Ley 25/2007) se establece el deber de retención de datos de tráfico relativos a las comunicaciones electrónicas en cuyo nº 3 nos dice 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, poniéndola a disposición de los jueces o tribunales o del Ministerio Fiscal que así lo requieran" . Finalmente la propia Agencia de Protección de Datos, órgano público de carácter autónomo que conforme al art. 37.1. a) de la L.O. 15/1999, 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, ha dicho en sus informes 135/2003 y 297/2005 que en los supuestos a que se refiere el art. 11.2 la cesión de datos personales no está sujeta a reserva jurisdiccional".*

**Un poco más cerca, quizás, de la realidad práctica…**

[24] Cuestionando incluso la decisión de la Audiencia Provincial correspondiente al decir que *"En atención a lo expuesto parece ser que la Audiencia confunde el derecho al secreto de las comunicaciones (art. 18-3 C.E.), el derecho a la intimidad (art. 18-1 C.E.) y la obligación de conservar secretos los datos informáticos personales (art. 18-4 C.E .) conforme a la Ley Orgánica de Protección de Datos de carácter personal, que excepciona la petición del Fiscal en el ejercicio de sus funciones legales de investigación de los delitos"* (fundamento jurídico quinto).

[25] Así dispone que *"El Mº Fiscal se hallaba en el ejercicio de sus funciones, entre otras, promover la acción de la justicia (art. 126 C.E. y art. 3 de su Estatuto Orgánico) y también investigando los hechos delictivos, dentro del marco de unas diligencias pre procesales de naturaleza criminal (art. 773-2 L.E.Cr)".* Y añade que *"Tal proceder del Mº Fiscal no afecta al secreto de las comunicaciones sino que se desenvuelve en el marco del derecho a la intimidad, más concretamente dada la escasa intensidad en que es efectuada, la cuestión se proyectaría sobre la obligación que establece la Ley Orgánica de Protección de Datos de no publicar los datos personales de los usuarios que un servidor de Internet posee, los cuales no pueden cederse sin el consentimiento del titular, pero la ley establece diversas excepciones".*

[26] En concreto se solicita a la operadora la identificación del usuario de una dirección IP y el número de teléfono de contacto a Internet, en el marco de una investigación penal de carácter pre-procesal.