EL DEBER DE CONSERVACIÓN DE DATOS EN LA UNIÓN EUROPEA Y SUS LÍMITES

INMACULADA LÓPEZ BARAJAS
Profesora Contratada Doctora de Derecho Procesal de la UNED

I. INTRODUCCIÓN

El punto de partida de este trabajo es la globalización, pues en este proceso de creciente integración de las distintas economías nacionales en una única economía de mercado mundial[1], han tenido una influencia decisiva las nuevas tecnologías de la información y de la comunicación.

La extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de comunicación, transmisión e intercambio de todo tipo

[1] wikipedia.org.

de información a gran velocidad ha originado profundos cambios y transformaciones sociales que han dado paso a la denominada «sociedad de la información»[2].

Se dice que se ha producido una auténtica «revolución tecnológica digital», de forma semejante a lo que sucedió con la Revolución Industrial en el siglo XIX.

Lo cierto es que la aplicación de las nuevas tecnologías 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 otros datos en soportes y formatos diversos.

Hasta hace pocas décadas el teléfono fijo era la única vía de telecomunicación al alcance real de la ciudadanía. Hoy se puede afirmar que las comunicaciones telefónicas clásicas han quedado superadas o, mejor dicho absorbidas, por las telemáticas o electrónicas.

Tradicionalmente, señala la doctrina[3], el término telemático ha supuesto la fusión de las técnicas de telefonía y tratamiento de datos (informática) y designa todo lo que tiene que ver con la comunicación entre ordenadores[4]. De hecho, ésta fue la expresión utilizada por el Legislador en diversas ocasiones para referirse a las comunicaciones, como por ejemplo en el artículo 544 ter de la Ley de Enjuiciamiento Criminal o en el artículo 197 del Código Penal.

Mas recientemente se observa una tendencia a sustituir el término tradicional de telecomunicaciones por el de comunicaciones electrónicas, cambio que, según una parte de la doctrina[5], se ha fundado en los cambios técnicos que se han producido, en concreto, en la digitalización de la información y convergencia de las comunicaciones que ha permitido un tratamiento homogéneo. Con este término se pone el acento en la forma de llevarse a cabo la comunicación y no tanto en la distancia superada.

II. EL DERECHO A ACCEDER LIBREMENTE A LA RED

Hecha esta precisión, una de las características básicas de la comunicación en Internet consiste en la existencia de mínimas barreras de entrada para la comunicación, tanto para emisores como para los receptores. Se tardan pocos minutos en dar de alta una cuenta de correo electrónico residenciada en un dominio situado al otro lado del mundo.

De hecho, el acceso a Internet constituye no solo un servicio sino un derecho que los poderes públicos deben garantizar y proteger. El derecho a acceder libremente a la red es hoy un derecho cuya titularidad corresponde a todas las personas.

---

[2] Corripio Gil-Delgado y Marroig Pol, L., *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones,* 2001, Madrid, p. 55.

[3] Losada, G., *Curso de Informática jurídica*, Tecnos, Madrid, 1987.

[4] Lázaro Laporta y Miralles Anguiñiga, *Fundamentos de telemática,* Valencia, 2002*,* p. 3.

[5] Hernández Guerrero, FJ, «La intervención de las comunicaciones electrónicas», en *Estudios Jurídicos del Ministerio Fiscal,* III, 2001, p. 347.

La Directiva 2002/22/CE, relativa al servicio universal y a los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas contempla hoy el acceso a Internet como parte del servicio universal de telecomunicaciones.

Pero la otra cara de la moneda, esto es, el reverso de todos estos aspectos positivos y, en concreto, de la facilidad de acceso que presentan las nuevas formas de comunicación electrónica es que ha sido utilizada por la delincuencia organizada para ampliar su infraestructura y potenciar la consecución de sus fines ilícitos.

Entre las notas que hoy caracterizan este tipo de delincuencia destaca su nivel de profesionalización y su carácter supranacional. Como ha señalado la doctrina[6] se trata de una delincuencia que se manifiesta de forma cada vez más violenta y más sofisticada en los medios y técnicas que utiliza para la comisión de hechos delictivos.

Este carácter supranacional se ha extendido a la delincuencia grave. Basta con observar la actividad jurisdiccional ordinaria que llevan a cabo los Jueces y Magistrados, donde se aprecia siempre un elemento transnacional en todos los delitos que tienen una cierta entidad.

Asimismo, el carácter anónimo y descentralizado de la red ha sido aprovechado por los criminales para comunicarse y cometer más delitos. Las nuevas tecnologías facilitan la perpetración del delito y dificulta su persecución.

La facilidad para generar nuevos dominios o accesos a la red, tanto localizados como remotos, han dejado anticuados los esquemas clásicos de actuación.

Así, para contrarrestar los sofisticados medios de que se sirven los grupos criminales organizados, así como el carácter internacional de su actividad, resulta necesario recurrir a nuevas técnicas de investigación[7].

Las autoridades encargadas de la prevención y persecución de los delitos han de contar con los medios de lucha adecuados para hacer frente a la delincuencia organizada que se sirve de las nuevas tecnologías.

Los tradicionalmente denominados datos de tráfico, entre los que se encuentran hoy los rastros o pistas técnicas de las comunicaciones electrónicas, han ido adquiriendo una importancia creciente, por su gran utilidad en la fase de investigación del proceso penal. A través de ellos podrá obtenerse información decisiva como la identidad de otros miembros de la organización criminal con los que mantiene conversaciones el imputado.

Esta utilidad unida al hecho de que se trata de datos que se difuminan enseguida, han sido los factores decisivos en el deber de conservación de estos datos que el legislador comunitario ha impuesto a las empresas de telecomunicaciones y servidoras de Internet.

---

[6] Magro Servet, V., «Intervención policial de mensajes sms y eficacia de las juntas provinciales de policía judicial», *Diario La Ley,* N. 6764. Jueves, 26 de julio de 2007.

[7] Zaragoza Aguado, «Tratamiento penal y procesal de las organizaciones criminales en el derecho español. Especial referencia al tráfico ilegal de drogas», en *Delitos contra la salud pública y el contrabando*, CGPJ, 2000.

III. EL RECONOCIMIENTO DEL DEBER DE CONSERVACIÓN DE DATOS DE LAS COMUNICACIONES ELECTRÓNICAS EN LA UNIÓN EUROPEA Y SU FUNDAMENTO

En un primer momento, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, reconoció la posibilidad de que los Estados miembros pudieran adoptar medidas legislativas que permitieran la conservación de datos durante un plazo limitado y justificado, siempre que fueren proporcionadas y necesarias en una sociedad democrática.

Asimismo, la Directiva 2000/31/CE, sobre servicios de la sociedad de la información y comercio electrónico, previó la obligación de comunicar a las autoridades competentes, a solicitud de estas, la información que les permitiera identificar a los destinatarios de su servicio con los que hubiesen celebrado acuerdos de almacenamiento.

En este marco, el Legislador español estableció en el art. 12 de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico 34/2002[8] el deber de retención de datos en el ámbito de Internet que afectaba a determinados prestadores de servicios de la sociedad de la información, por estar directamente vinculados a ellos los rastros electrónicos que dejan los usuarios a través de la red[9]. Esta especialidad fue recogida posteriormente por la Ley General de Telecomunicaciones 32/2003, de 3 noviembre.

Las investigaciones llevadas a cabo en diversos estados miembros, especialmente en el ámbito de la delincuencia organizada, han puesto de manifiesto la gran utilidad del tratamiento de los datos relativos al uso de las comunicaciones electrónicas que se erigen, por tanto, en una herramienta muy valiosa en la prevención, investigación y enjuiciamiento de delitos, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo.

Por ello, se ha optado por armonizar las legislaciones nacionales a través de la Directiva 2006/24/CE, de 15 de marzo, 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, por la que se modifica la Directiva 2002/58/CE en el sentido de distinguir entre la obligación de retención que específicamente establece la nueva Directiva, de la mera posibilidad de retención de aquellos datos que quedan fuera de su ámbito de aplicación.

---

[8] El art. 12, derogado por la Ley 25/2007, disponía que «los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo».

[9] Ballesteros Moffa, L.A., «Hacia un difícil equilibrio entre privacidad y seguridad…, *op. cit.,* p. 44.

Como no podía ser de otra manera, en el reconocimiento legal de esta obligación ha tenido una influencia decisiva la magnitud de los atentados acontecidos en la última década (Nueva York, Madrid y Londres) que ha fortalecido la voluntad del Consejo de Europa de luchar contra todas las formas de terrorismo, expresando este firme propósito de la Unión en un amplio catálogo de medidas, entre las que se encontraba la retención de datos de tráfico de las comunicaciones electrónicas.

Este «Nuevo terrorismo internacional» se caracteriza por el carácter global de la amenaza que supone.

Ahora bien, aunque el motor de la regulación comunitaria sobre la disponibilidad de los datos almacenados relativos a las comunicaciones electrónicas se inspiraba en la necesidad de perseguir el terrorismo y la delincuencia organizada, finalmente la Directiva 2006/24/CE ha optado por la fórmula abierta de delito grave según la legislación interna de los Estados miembros.

Así, el fundamento de este deber se encuentra en la necesidad de garantizar el mantenimiento de unos datos con vistas a su eventual utilización en el marco de un proceso penal.

Con esta medida, se trata de reforzar los instrumentos a disposición de las Fuerzas y Cuerpos de Seguridad de los Estados para el ejercicio de las funciones de seguridad pública que tienen atribuidas, permitiendo que puedan acceder a ciertos datos que, hasta entonces, no solían estar disponibles.

Asimismo, supone un pequeño paso adelante en el largo camino de la aproximación de las legislaciones procesales de los Estados miembros, que es la base para que pueda funcionar bien la cooperación policial y judicial en materia penal, que a su vez es fundamental para configurar la Unión como un espacio de libertad, seguridad y justicia, uno de los objetivos centrales de las reformas que lleva aparejado el Tratado de Lisboa.

IV. LÍMITES PREVISTOS EN LA DIRECTIVA 2006/24/CE, DE 15 DE MARZO

Pero, el establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, debe efectuarse buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la inviolabilidad de de las comunicaciones.

Para ello, la Directiva 2006/24/CE establece una serie de garantías. La primera se centra en los fines del deber impuesto a las empresas de telecomunicaciones. La segunda se refiere al tipo de datos que pueden ser objeto de conservación y posterior cesión. La tercera se concreta en la autoridad competente para acceder a los datos que han sido previamente conservados. De todas ellas pasamos a ocuparnos a continuación, para posteriormente analizar la nueva normativa a la luz del respeto a los derechos fundamentales y a los principios básicos del Derecho Penal y del proceso debido.

1. La exclusividad de los fines del deber de conservación

Tal y como dispone la Directiva 2006/24/CE los datos sólo pueden ser objeto de conservación para los fines exclusivos que la misma establece, y que consisten en *la detección, investigación y enjuiciamiento* de delitos graves definidos éstos de acuerdo con la legislación interna de cada Estado miembro. En nuestro Derecho, se consideran de esta naturaleza aquéllos para los que se establezcan penas privativas de libertad superiores a cinco años.

Conviene recordar que, como se indicó mas arriba, aunque el motor de la regulación comunitaria sobre la disponibilidad de los datos almacenados relativos a las comunicaciones electrónicas se inspiraba en la necesidad de perseguir el terrorismo y la delincuencia organizada, el legislador comunitario finalmente ha optado por la fórmula más amplia de delito grave.

De esta manera, se pueden obtener los datos relativos a las comunicaciones que puedan estar relacionados con una investigación penal de un delito grave, y que se hayan efectuado por medio de la telefonía fija o móvil, así como a través de Internet.

Queda prohibida la conservación con otras finalidades como la cesión con fines comerciales, como por ejemplo para la oferta de bienes o servicios determinados en función de las preferencias que los sujetos hayan manifestado en su tráfico comunicativo[10].

A nadie se le escapa que la observación y tratamiento irregular de estos datos permitiría conocer e interpretar el comportamiento del usuario, configurándose a partir de ellos perfiles sobre sus gustos, preferencias o hábitos personales, e incluso sobre creencias religiosas, ideas políticas o aspectos privados de la salud.

En definitiva, las nuevas tecnologías de la comunicación y de la información permiten conocer la forma de ser y de comportarse de las personas.

Por ello, desde las primeras Leyes sobre telecomunicaciones el legislador ha tratado de establecer una regulación específica protectora conforme a la cual los datos o huellas electrónicas deben eliminarse o convertirse en anónimos una vez que dejen de ser necesarios para la transmisión de la comunicación, salvo a efectos de facturación o pago.

Pero, en el caso que nos ocupa, como ha señalado la doctrina[11], al deber general de eliminación de esta clase de datos tras el cumplimiento de su función, se ha superpuesto al deber de retención de los mismos con fines de seguridad.

---

[10] Moreno Catena, V., «Ley de conservación de datos y garantías procesales», en AAVV *La protección de datos en la cooperación policial y judicial,* Thomson-Aranzadi, 2008, p. 163 y ss.

[11] Ballesteros Moffa, LA., «Hacia un difícil equilibrio entre privacidad y seguridad: la conservación de datos en las comunicaciones electrónicas y la transferencia de datos de pasajeros por las compañías aéreas», *REDA*, Thomson-Civitas, marzo, 2008.

2. Ámbito objetivo

El segundo límite se extiende al tipo de datos que pueden ser objeto de conservación. Así, el deber de retención se extiende tanto a la telefonía fija y móvil, como al ámbito de Internet, correo electrónico o telefonía por Internet.

Se trata de conservar los datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta.

La Directiva 2006/24/CE exige que se conserven exclusivamente los datos generados o tratados en el proceso del suministro de servicios de comunicación. De esta manera, cuando dichos datos no hayan sido generados o tratados por dichos proveedores, no es obligatorio conservarlos. Esto es, el deber se refiere únicamente a los datos ya tratados por los proveedores a los efectos de hacer posible la comunicación o los servicios vinculados a ella.

Sólo se conservarán los datos necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos (nombre y dirección), los que permiten determinar el momento (la hora y fecha) y duración, el tipo de servicio y el equipo de comunicación utilizado por los usuarios que, cuando se trate de un equipo móvil, también abarcará los datos necesarios para su localización.

Ha precisado la doctrina[12], que la expresión «servicio de Internet utilizado», en el caso de correo electrónico por Internet y telefonía por Internet, debe ser entendida como comprensiva únicamente de los instrumentos utilizados para la comunicación (mensaje de correo electrónico, videoconferencia por Internet etc), pues de otro modo se estaría produciendo una injerencia sobre el contenido de la comunicación.

Por tanto, el objeto del deber de conservación se circunscribe, básicamente, a los datos que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones.

A continuación, la Directiva 2006/24/CE enumera en su artículo 5, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en los tres ámbitos mencionados, telefonía fija, móvil o Internet. Destacamos a continuación los aspectos más significativos y novedosos.

En cuanto a los datos necesarios para identificar el equipo de comunicación de los usuarios: 1) con respecto a la telefonía de red fija se incluyen los necesarios para identificar el número de origen y destino de la comunicación 2) con respecto a la telefonía móvil comprende, además de los números de teléfono de origen y destino, la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada y de la parte que recibe la llamada y la identidad internacional del equipo

---

[12] Rodríguez Lainz, JL, «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», *Diario La Ley*, Nº 6859, Sección Doctrina, 11 enero 2008, Año XXIX.

móvil (IMEI) de la parte que efectúa la llamada y de la parte que recibe la llamada; 3) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet se incluyen el número de teléfono de origen en caso de acceso mediante marcado de números, y la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

Como novedad, quedan incluidas también en el ámbito de aplicación del deber de conservación las denominadas llamadas telefónicas infructuosas o perdidas. Éstas constituyen un intento de comunicación que a pesar de no tener éxito porque el receptor no atiende la llamada, sin embargo reflejan un indicio de relación entre personas investigadas.

La Directiva 2006/24/CE habla de la «llamada telefónica infructuosa» y la define como una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación toda vez que ha habido una intervención por parte del gestor de la red. De esta manera, queda clara la distinción entre las llamadas perdidas y las no conectadas, con respecto a las cuales no es obligatoria, sin embargo, la conservación de datos.

En la transposición de la Directiva analizada al Ordenamiento español, también se incluye como novedad, la obligación de conservar los datos necesarios para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

Así, la Ley 25/2007, de 18 de octubre, de conservación de datos de comunicaciones electrónicas y de redes públicas de comunicación, que implementa la Directiva, impone un deber de identificación cuando se adquieran las tarjetas prepago de telefonía móvil, imponiendo la obligación de llevanza de un libro registro de los adquirentes de este tipo de tarjetas.

Aunque la obligación de inscripción se exige desde la entrada en vigor de la Ley (noviembre de 2007), se establece un régimen transitorio para las tarjetas adquiridas con anterioridad. Así, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, para cumplir con las obligaciones de inscripción. Transcurrido dicho período de tiempo sin haber sido posible el registro, tienen el deber de anularlas o desactivarlas, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

La doctrina ha puesto de manifiesto que esta exigencia debería haberse hecho extensiva a todos los servicios anónimos de pago por adelantado.

Un caso claro es el de los cibercentros, donde el usuario accede a Internet sin ningún tipo de control. De hecho, en el debate parlamentario de la Ley se presentó una enmienda con objeto de proponer la llevanza de un libro registro de los usuarios que acceden a Internet a través de sus ordenadores, de manera semejante a los vendedores de las tarjetas de telefonía prepago.

De todo lo expuesto resulta que el ámbito del deber de conservación impuesto por la Ley 25/2007 de 18 de octubre, abarca un conjunto heterogéneo de datos que se almacena para su eventual utilización posterior y que, pese a su diferente naturaleza, se someten a un régimen jurídico común.

3. Ámbito subjetivo

Según la Directiva 2006/24/CE los datos conservados solamente se pueden facilitar a las autoridades nacionales competentes de conformidad con la Legislación nacional, respetando plenamente los derechos fundamentales de las personas afectadas.

La Ley 25/2007 que transpone la Directiva exige para que sea válida la cesión de los datos que concurra siempre autorización judicial previa. A continuación, dispone que la información debe facilitarse por los sujetos obligados a los agentes facultados.

Los sujetos obligados son los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

Por su parte, el Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas, define al operador como la persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad.

Por último, en cuanto a los agentes facultados, la Ley los define como los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de Policía judicial, de acuerdo con lo previsto en el artículo 547 de la LOPJ.

También tendrán esta consideración los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como Policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

Por último, también se consideran agentes facultados para recibir los datos conservados, el personal del Centro Nacional de Inteligencia cuando actúen en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia.

De esta manera, es la autoridad judicial la que autoriza siempre y ordena la cesión de los datos habilitando a los agentes facultados para que recaben de los operadores obligados la información que han sido previamente conservados.

4. Plazo del deber de conservación

En cuanto a los plazos de esta obligación de conservación, la Directiva 2006/24/CE establece un período de tiempo que no sea inferior a 6 meses y un máximo de 2 años.

Dentro de este marco, el legislador español ha fijado un plazo general de conservación de doce meses desde que la comunicación se hubiera establecido, que reglamentariamente se podrá reducir a seis meses o ampliar a dos años, atendiendo al

coste de almacenamiento y conservación de los datos, así como al interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

V. LÍMITES DERIVADOS DEL RESPETO AL CONTENIDO ESENCIAL DE LOS DERECHOS FUNDAMENTALES

Tal y como se mencionó más arriba, el establecimiento de este deber de conservación de datos, justificado en aras de proteger la seguridad pública, debe efectuarse buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la inviolabilidad de de las comunicaciones.

La doctrina[13] llama la atención sobre la necesidad de ponderar despacio las injerencias en la esfera de los derechos fundamentales, aun en el caso de que estén previstas en la Ley, para que no se desvirtúe el contenido esencial de los derechos fundamentales afectados tal y como se reconocen por la norma Constitucional.

Por ello, resulta oportuno analizar si la nueva normativa, como medio de confrontación para lograr la represión eficaz de estas nuevas formas de delincuencia, se produce dentro del respeto a los principios básicos del Derecho Penal y del proceso debido.

La obligación de conservación y el deber de cesión de los datos retenidos debe producirse dentro de los límites autorizados por el Convenio Europeo sobre Derechos Humanos. De conformidad con la interpretación del TEDH, toda injerencia de las autoridades públicas en el derecho a la vida privada debe respetar los principios de necesidad y de proporcionalidad

1. Delimitación de los Derechos fundamentales afectados

La propia Directiva 2006/24/CE, en su considerando 22, se refiere expresamente al respeto de la vida privada y de las comunicaciones y a la protección de los datos de carácter personal, que se consagran en los art. 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Nos encontramos, pues, ante tres derechos fundamentales íntimamente relacionados: el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos frente al uso de la informática, también denominado derecho a la autodeterminación informativa.

Aunque se trata de derechos conexos resulta necesario proceder a su delimitación toda vez que se están sujetos a un régimen jurídico diferente.

---

[13] Moreno Catena, V., «Ley de conservación de datos y garantías procesales», en AAVV *La protección de datos en la cooperación policial y judicial,* Thomson-Aranzadi, 2008, pp. 163 y ss.

2. El derecho al secreto de las comunicaciones

El secreto de las comunicaciones se reconoce como garantía en todas las Constituciones, así como en las normas internacionales, entre otras, en la Declaración Universal de Derechos Humanos[14] y en el Pacto Internacional de Derechos Civiles y Políticos[15].

En nuestro texto constitucional se reconoce en el art. 18.3, y por tanto con rango de derecho fundamental, según el cual «*se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*».

Por su parte el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de forma más amplia establece, que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

En lo que a las comunicaciones electrónicas se refiere el art. 33 de la Ley General de Telecomunicaciones establece que los operadores que exploten redes públicas de comunicaciones o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

Por su parte, el art. 5.2 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas, dispone que los operadores no podrán acceder a la línea de un usuario final sin su consentimiento expreso e inequívoco.

A. El carácter formal del derecho

El derecho al secreto de las comunicaciones garantiza a los interlocutores o comunicantes una protección que se proyecta sobre el proceso de comunicación mismo con independencia de que el contenido del mensaje transmitido pertenezca o no al ámbito de lo personal, lo íntimo o lo reservado (STC 114/1984). De esta forma, el objeto de este derecho es la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado (STC 123/2002). Toda comunicación es para la norma fundamental secreta aunque sólo algunas sean íntimas. No se dispensa del secreto en función del contenido de la comunicación.

El constituyente español no ha querido proteger exclusivamente el secreto de las comunicaciones «íntimas», sino cualquier clase de comunicación, con indepen-

---

[14] Art. 12 «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques».

[15] Art. 17 «1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y su reputación. 2. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques».

dencia de su contenido. Esto otorga una dimensión formal al derecho que se contrapone con la dimensión material del derecho a la intimidad[16].

Tanto el TEDH como nuestro TC han afirmado este carácter formal del derecho al secreto de las comunicaciones. De esta manera, a pesar de nuestra sistemática constitucional, que parece conectar el derecho al secreto de las comunicaciones con el derecho a la intimidad, queda clara la autonomía y sustantividad del derecho al secreto de las comunicaciones con independencia de que el contenido de lo comunicado incida en la esfera de lo íntimo.

El fundamento de este carácter autónomo y separado del reconocimiento de este derecho fundamental y de su específica protección 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 (STC 123/2002).

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), se proyecta sobre su régimen jurídico. Así, mientras *ex* art. 18.3 CE la intervención de las comunicaciones requiere siempre resolución judicial, no existe en la Constitución reserva jurisdiccional absoluta respecto del derecho a la intimidad personal, donde se ha admitido, de forma excepcional, que en determinados casos y, con la suficiente y precisa habilitación legal, es posible que la Policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas[17].

Además, en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo una garantía de la libertad individual, sino que se erige, asimismo, en la garantía para el ejercicio de múltiples derechos y libertades como la propiedad, el secreto del sufragio activo, la libertad de opinión, ideológica y de pensamiento, de la libertad de empresa, la confidencialidad de la asistencia letrada, etc.

B. Los nuevos datos de tráfico y el principio de la menor intensidad en la injerencia

El carácter eminentemente formal del derecho al secreto de las comunicaciones impide modulaciones o grados de actuación, de tal forma que la incidencia no consentida por un tercero en el ámbito de lo que deba entenderse como objeto del derecho al secreto de las comunicaciones, supone una infracción del mismo de alcance constitucional (STC 123/2002).

---

[16] Moreno Catena, V., *Garantía de los derechos fundamentales en la investigación penal,* Poder Judicial, 1987, p. 155.

[17] Gimeno Sendra, V., *Derecho Procesal Penal,* Colex, Madrid, 2004; «Las intervenciones telefónicas en la jurisprudencia del TC y TS», en *Estudios jurídicos en homenaje al profesor Aurelio Menéndez,* Civitas, Madrid; *Los procesos penales. Comentarios a la Ley de Enjuiciamiento Criminal con formularios y jurisprudencia,* Tomo IV, Bosch, Barcelona, 2000.

Para delimitar el objeto del derecho, resulta obligado tomar como punto de partida la citadísima sentencia del Tribunal Europeo de Derechos Humanos en el caso Malone contra Reino Unido de 2 de agosto de 1984, según la cual el concepto del secreto de la comunicación no sólo cubre su contenido sino que alcanza a todos los aspectos de la misma, como por ejemplo, la propia existencia de la comunicación, la identidad subjetiva de los interlocutores, 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.

Así, y dado que el bien constitucionalmente protegido es la libertad de las comunicaciones, la jurisprudencia del Tribunal Europeo de Derechos Humanos reconoce expresamente la posibilidad de que el art. 8 de la Convención pueda resultar violado por el empleo de un artificio técnico que permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma (STC 56/2003).

En definitiva, no cabe disociar, sin merma relevante de garantías, realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

Resulta claro que los datos de tráfico permiten conocer algunos extremos relativos a la comunicación como el momento y la duración. También permiten conocer aspectos de gran relevancia como la identidad de las personas que establecen el contacto, y precisamente por eso, puede sostenerse que forman parte, auténticamente, del contenido de la comunicación[18].

Pero, hoy en día la telefonía móvil y la telefonía a través de Internet generan 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 24 años.

Estos nuevos datos aportan valiosa información sobre el origen de la comunicación, lo que permitirá, en la mayor parte de los casos, ubicar el equipo informático desde el que se ha llevado a cabo la comunicación, el momento de la misma, así como la identificación de un abonado titular de la línea de conexión a través de la cual se accede a Internet, aunque no al usuario de la misma[19].

En este nuevo concepto de datos de tráfico se incluyen elementos de una naturaleza y funcionalidad heterogénea. El problema consiste en delimitar bien los datos concretos a los que debe extenderse el secreto, diferenciándolos de aquéllos que forman parte del contenido del derecho a la protección de datos o de los que deberían protegerse a través del derecho a la intimidad.

---

[18] Por ello, cuando, en un caso, lo que la Policía lleva a cabo no es identificar los números telefónicos en comunicación, sino, tan sólo, averiguar el correspondiente a uno de los comunicantes, no puede afirmarse con propiedad que se esté interviniendo en esa comunicación, dado que la comunicación, por definición, requiere, al menos, dos comunicantes y, por tanto, la actuación sobre un solo individuo y los objetos de su pertenencia nunca puede constituir injerencia en sus comunicaciones ni, menos aún, en las de un tercero (voto particular de STS 130/2007, de 19 de febrero).

[19] Salom Clonet, J., «Incidencia de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos», *op. cit.,* p. 136 y ss.

Esta tarea resulta, en ciertas ocasiones, compleja. Ha señalado una parte de la doctrina[20] que la incidencia de los diferentes regímenes es tal que pueden llegar a confluir.

Han sido los avances tecnológicos y la aparición de las nuevas técnicas de investigación basadas en el análisis de los datos de tráfico de las comunicaciones las que han dado lugar a una cierta evolución en la jurisprudencia del Tribunal Constitucional que, al proclamar el principio de menor intensidad en la injerencia, reconoce una menor exigencia constitucional en el respeto al derecho constitucional afectado que, no por ello, deja de estar situado dentro del ámbito del derecho al secreto de las comunicaciones garantizado por el 18.3 CE.

Este principio de la menor intensidad en la injerencia se plasma en la STC 26/2006 donde se autoriza una investigación basada en el listado de llamadas, pero no una injerencia sobre los contenidos dado el carácter impreciso de los indicios alegados por la Policía Judicial. Esto es, sin negar la existencia de indicios, el órgano jurisdiccional no los consideró suficientes para realizar una intervención total de las comunicaciones, pero sí para conocer la identidad de los interlocutores.

Por ello, la intervención de los datos de tráfico puede acordarse como una diligencia previa a la intervención del contenido material que, con base en la menor lesividad para el derecho afectado, puede superar más fácilmente el juicio de necesidad (STS 1476/2005, de 25 de noviembre)[21].

Con base en las consideraciones expuestas, algunos autores[22] defienden la autonomía de la intervención de los datos de tráfico con respecto a la intervención del contenido material. De esta forma, el primer tipo de intervención podría adoptarse, además de para localizar o establecer vínculos entre sospechosos, con vistas a determinar si procede la intervención del contenido material. Por ello, proponen que podría fundarse en la investigación de delitos de menor entidad.

Pero a día de hoy, el TC no ha ido tan lejos, aunque sí ha dicho que los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE (STC 70/2002).

3. El derecho a la protección de datos de carácter personal

Otro derecho que cobra especial relieve en el ámbito de las comunicaciones electrónicas es el derecho a la protección de datos de carácter personal también lla-

---

[20] Rodríguez Lainz, J.L., *Intervención judicial en los datos de tráfico de las comunicaciones,* Bosch, Barcelona, 2003, pp. 447 y ss.

[21] González López, *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal,* La Ley, 2007, p. 167.

[22] González López, *Los datos de tráfico de las comunicaciones, op. cit.,* p. 168.

mado derecho a la autodeterminación informativa[23], reconocido en el art. 18.4 de nuestro texto constitucional.

Se trata de un derecho que, con el tiempo, ha adquirido un estatus jurídico propio y ha sido reconocido con el rango de derecho fundamental (STC 292/2000). Se regula, en nuestro Derecho positivo, por la Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y, en el ordenamiento comunitario por la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, y por la Directiva 2002/58/CE relativa la tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

La libertad informática ha sido calificada por algunos autores[24] como un derecho fundamental propio de la actual sociedad de la información en la que estamos inmersos.

El derecho a la protección de datos de carácter personal, está íntimamente ligado al derecho al secreto de las comunicaciones. Por ello, la delimitación o frontera de los mencionados derechos tiene gran importancia, con objeto de fijar el régimen jurídico al que deben adscribirse los datos de tráfico, y en consecuencia las garantías para que sea lícita su utilización en cada caso.

Así, a juicio del Tribunal Constitucional, el derecho fundamental a la protección de datos, comparte con el derecho a la intimidad el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, si bien se diferencia del mismo en dos aspectos fundamentales.

En primer lugar, el objeto de protección del derecho fundamental a la protección de datos es mas amplio toda vez que no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

Su protección se extiende a todos aquellos datos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo

La segunda peculiaridad que posee el derecho fundamental a la protección de datos y que la distingue del derecho a la intimidad personal y familiar del art. 18.1 CE radica en su contenido, ya que a diferencia de este último, que confiere a la per-

---

[23] Martín Retortillo Baquer, L., «Consideraciones comunes a los artículos 49, 50 y 51 de la Ley General de Telecomunicaciones», en AAVV, *Comentarios a la Ley General de Telecomunicaciones,* Civitas, Madrid, 1998, p. 428.

[24] Olover Lalana, D., «El derecho fundamental virtual a la protección de datos. Tecnología transparente y normas privadas», Diario La Ley, núm. 5592, de 22 de julio de 2002.

sona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular la facultad de imponer a terceros deberes jurídicos. Por ejemplo, el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de control y disposición sobre los datos personales (STC 254/1993, F.J. 7).

De todo lo expuesto se deduce que el derecho fundamental a la intimidad (art. 18.1 CE) no aporta por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico, dadas las amplísimas posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales.

Una vez delimitado el ámbito del derecho a la protección de datos respecto al derecho a la intimidad, procede ahora, delimitarlo con relación al derecho al secreto de las comunicaciones.

Para ello, resulta necesario atender al aspecto dinámico o estático de la comunicación. En el primer caso, esto es, mientras dura el proceso de comunicación, quedará afectado el derecho al secreto de las comunicaciones, ya incida la injerencia sobre el contenido de la comunicación o sobre sus elementos externos o adyacentes. En cambio, cuando la comunicación se ha consumado, se almacenan en una base los datos relativos a las comunicaciones, y pasan a configurarse como datos de carácter personal.

Así, los datos del emisor y receptor de una comunicación, una vez finalizada ésta ya no deben protegerse por el derecho fundamental al secreto de las comunicaciones, a pesar de su estrecha conexión con la comunicación realizada, sino a través de las normas que regulan la intimidad u otros derechos, toda vez que no suponen una interferencia en un proceso de comunicación (STC 70/2002).

Así, la entrega por la operadora del listado de las llamadas ya ejecutadas con anterioridad desde un determinado número de teléfono no afecta al contenido propio del derecho al secreto de las comunicaciones, toda vez que se trata, en definitiva, de datos de carácter personal, custodiados en ficheros automatizados, a que se refiere la Ley Orgánica 5/1992, de 29 de octubre, Reguladora del Tratamiento de tales datos, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución estableciéndose en la misma que el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, el cual, sin embargo, no será preciso cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas.

De hecho, tal información, propia de la investigación judicial en la fase de instrucción, es similar a la relativa al movimiento de las cuentas corrientes bancarias, y no afecta en forma alguna al secreto de las comunicaciones telefónicas. El registro de las llamadas efectuadas desde un determinado número de teléfono forma parte del conjunto de datos que las correspondientes compañías telefónicas obtienen y

conservan para poder determinar el precio que periódicamente debe abonarles el titular de aquél, al cual se le facilitan, bien espontáneamente, bien previa solicitud, para su conocimiento y posibles reclamaciones; en forma semejante a como hacen las entidades bancarias con los titulares de las cuentas corrientes, al remitirles periódicamente información sobre el movimiento de las mismas (STS 459/1999). En análogo sentido se manifiesta la STS de 7 de diciembre de 2001, F2, RJ 2002/2070.

La Agencia Española de Protección de Datos ha reconocido conforme con la normativa de protección de datos la cesión de datos reservados de carácter personal a petición de la Policía judicial, esto es, sin mediar resolución judicial previa, cuando se trate de datos necesarios para la prevención y represión de determinados delitos graves, siempre que estén debidamente motivados y se comunique inmediatamente a la autoridad judicial.

4. Consecuencias prácticas de la delimitación

Ante la confluencia de tantos derechos implicados, Ley 25/2007, de 18 de octubre que traspone la Directiva 2006/24/CE al ordenamiento español, en vez de delimitar el régimen jurídico de la conservación y cesión en función del tipo de datos a retener, corta por lo sano, esto es, exige autorización judicial para la cesión de todos los datos cualquiera que sea su naturaleza.

Por ello, corresponde siempre al Juez decidir sobre el hecho de la cesión y sobre el contenido de lo que ha de cederse en función de los principios de necesidad y proporcionalidad de la medida, de modo semejante a como se exige para la intervención de las comunicaciones telefónicas (art. 7.2 LCDCE). Sólo así la utilización de estos datos puede tener eficacia probatoria en el proceso penal.

Esto ha provocado que desde el primer momento de aplicación de la nueva Ley, se hayan suscitado importantes dudas sobre el régimen que debe informar la obtención de ciertos datos por la Policía Judicial. Esto es, sobre la necesidad de someter a autorización judicial la captación de ciertos datos que, a pesar de estar incluidos dentro del ámbito objetivo de la nueva Ley de Conservación de Datos, pueden ser obtenidos directamente por la Policía.

Así ocurre con la obtención de las claves IMSI (*Internacional Mobile Subscriber Identity* - Identidad Internacional del Abonado a un Móvil) e IMEI, y con la obtención de los protocolos de acceso a Internet. A través de estos supuestos se puede comprender mejor las importantes consecuencias prácticas que tiene la delimitación del tipo de derecho afectado en cada caso, toda vez que marca la frontera de la investigación policial en la materia, la cual no puede afectar al núcleo protegido por el derecho fundamental al secreto de las comunicaciones sin que medie autorización judicial.

A. La obtención de las claves IMSI e IMEI

Una consideración especial merece el estudio de los datos IMSI e IMEI por la gran polémica jurisprudencial que se ha generado a propósito del régimen jurídico que debe informar su obtención por la Policía Judicial.

El IMSI es una relación alfanumérica vinculada a una tarjeta SIM. El IMEI es un código vinculado a un teléfono móvil GSM y que, por tanto, identifica un terminal de telefonía móvil.

La técnica consistente en la identificación de estos códigos (IMSI e IMEI) ha sido definida como un procedimiento que permite detectar las claves de los teléfonos móviles que llevan las personas que se encuentran a determinada distancia mediante el rastreo del espacio radioeléctrico. Se basa en la existencia de un teléfono operativo, sin necesidad de que se esté siendo utilizado en ese momento.

Sobre su posible inclusión dentro del ámbito del art. 18.3 existen dos posiciones. La primera entiende que supone una intromisión en el derecho al secreto de las comunicaciones en la medida en que, por una vía más indirecta (la del código del terminal), se puede obtener el mismo efecto de invasión del ámbito del secreto (SSTS de 23 de enero de 2007 y de 19 de febrero de 2008). En el mismo sentido, una parte de la doctrina[25] considera que se trata de una técnica equivalente al recuento del que trataba el caso Malone, y por tanto, necesitada de autorización judicial. Precisa Rodríguez Lainz que en el actual estado de la técnica el IMSI sólo puede captarse o durante el proceso de autenticación o en el tránsito de señales automáticas para actualizar la ubicación geográfica del terminal cada vez que cambia de estación. Por ello, el mencionado autor, aun reconociendo que se trata de operaciones automáticas, ajenas a la voluntad del usuario, considera que en ambos casos se trata de comunicación.

La segunda posición entiende, sin embargo, que se trata de una técnica que no afecta al núcleo protegido por el art. 18.3 CE, toda vez que la obtención de esta información, por sí sola, no permite conocer la identidad de los comunicantes, ni la titularidad del teléfono móvil, ni dato alguno sobre el tráfico de llamadas entrantes o salientes del sospechoso. Además, esa numeración puede llegar a aprehenderse, incluso, sin necesidad de que el proceso de comunicación se halle en curso. Con ello quiebran las ideas de funcionalidad y accesoriedad, de importancia decisiva a la hora de calificar jurídicamente el alcance de la tutela constitucional de esa información.

De hecho, estos identificadores, aisladamente considerados, no aportan información significativa, sino tan solo cuando se analizan junto a los datos contenidos en las bases de datos de las operadoras de telefonía, para lo cual se necesita siempre la correspondiente autorización judicial.

Por ello, el voto particular de la STS de 23 de enero de 2007 entendió que los mencionados números identificativos con los que operan los terminales no pueden constituir, por sí mismos, materia amparada por el secreto de las comunicaciones, pues afirmar lo contrario supondría, confundir los medios que posibilitan la comunicación con la comunicación misma.

Asimismo, el mencionado criterio no supone contradicción alguna, con la doctrina del Tribunal Europeo de Derechos Humanos, significativamente la contenida

---

[25] Rodríguez Lainz, J.L., «Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas», *Diario La Ley*, num. 7886, 2009.

en la Sentencia del denominado «caso Malone» (TEDH 1984, 1), ni con la del Tribunal Constitucional ni, mucho menos aún, con la de la propia Sala segunda del Tribunal Supremo, pues esa doctrina se refiere a la extensión del ámbito protegido de la «comunicación» no tanto a los números telefónicos sino al hecho de que, a través de la averiguación de esos números, se conozcan extremos como el momento, la duración y, lo que es aún más importante, la identidad de las personas que establecen el contacto. Estas circunstancias sí que puede sostenerse que forman parte, auténticamente, de la «comunicación».

Por ello, cuando lo que la Policía lleva a cabo no es identificar los números telefónicos en comunicación, sino, tan sólo, averiguar el correspondiente a uno de los comunicantes, no puede afirmarse con propiedad que se esté interviniendo en esa comunicación, dado que la comunicación, por definición, requiere, al menos, dos comunicantes y, por tanto, la actuación sobre un solo individuo y los objetos de su pertenencia nunca puede constituir injerencia en sus comunicaciones ni, menos aún, en las de un tercero.

Ahora bien, el hecho de que esta 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, no excluye que su tratamiento automatizado no implique un significativo nivel de injerencia en la privacidad del interesado ya que interrelacionado con otros datos en poder del operador puede dar lugar a conocer, entre otros datos, la identidad del comunicante.

Por ello, podría considerarse como un dato de carácter personal a la luz de la lectura del art. 3.a) de la LO 15/1999, de Protección de Datos de Carácter Personal, con arreglo al cual, dato personal es cualquier información concerniente a personas físicas identificadas o identificables.

La mencionada Ley 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. A continuación, 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 (art. 11.2.d).

Ello no obstante, no debe olvidarse que la Ley de Conservación de Datos menciona a los datos IMSI e IMEI (art. 3.1 e)), para cuya cesión resulta exigible la misma regla impuesta al resto de los datos a los que se refiere, que requiere la preceptiva autorización judicial. Con esta especial protección podría parecer que el legislador los está considerando como parte del derecho al secreto de las comunicaciones[26].

Sobre esta cuestión se ha pronunciado la STS 249/2008, de 20 de mayo según la cual debe distinguirse el supuesto de cesión de la información sobre el IMSI des-

[26] Ortiz Navarro y Lucas Martín, «Ámbito de protección del derecho al secreto de las comunicaciones», *op. cit.,* p. 34.

de los ficheros automatizados que obran en poder de los prestadores de servicio (regulada por la Ley 25/2007), del acceso a esta información desde el propio teléfono celular por las Fuerzas y Cuerpos de Seguridad del Estado, sobre la nada dice la Ley de Conservación de Datos.

Así, frente al silencio de la nueva regulación, podría resultar de aplicación lo dispuesto en la Ley de Protección de Datos 15/1999, según la cual 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 estos datos, 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).

Ello no obstante, la facultad de recogida de datos que la LO 15/1999 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 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).

Teniendo en cuenta que el IMSI, por sí solo, no un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos, según la mencionada sentencia, su recogida o captación técnica 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 requerirá el control jurisdiccional de su procedencia.

En el mismo sentido se ha pronunciado la posterior STS 776/2008, de 18 de noviembre según la cual la averiguación de las claves alfanuméricas, cuando se lleva a cabo en el marco de una investigación criminal relativa a un delito de especial gravedad, difícilmente puede considerarse que suponga una indebida y desproporcionada restricción de un derecho fundamental y que, por ello, suponga una vulneración constitucional con sus lógicas consecuencias (v. art. 11.1 LOPJ).

Los mismos argumentos se recogen en los siguientes pronunciamientos del TS que sostienen que los IMSI pueden ser obtenidos por los agentes policiales por sus propios medios sin que ello acarree nulidad alguna de las pruebas obtenidas ya que no entran en el ámbito de la privacidad de las comunicaciones.

Incluso la jurisprudencia ha ido más allá. La reciente STS 40/2009, de 28 de enero considera que el IMSI y el IMEI difícilmente pueden considerarse datos de carácter personal. De hecho, la doctrina especializada suele entender que el IMSI, desde el punto de vista pericial, equivale a una labor de vigilancia convencional, en la que se determina con quién se encuentra el vigilado, con quién habla, por dónde se desplaza o qué objetos toca; o bien cuál es el domicilio de una persona, para cuya entrada y registro se solicitará, en su momento, el pertinente mandamiento judicial. Así, considera que de la misma manera que se puede ver en una vigilancia (mediante prismáticos, por ejemplo) la marca y modelo del teléfono móvil que utiliza un vigilado, se puede obtener la información del IMSI, mediante estos «prismáticos especiales inalámbricos».

De lo expuesto se deduce la existencia de una jurisprudencia reiterada favorable a la actuación directa de la Policía en esta materia. Ello no obstante, dado que, en un principio existieron criterios cambiantes, en la práctica, la Policía Judicial suele acudir a la autoridad judicial para que autorice el uso del interceptador o, cuando menos, para informarle previamente sobre su intención de utilizarlo. De esta manera, evitan incurrir en responsabilidad por vulnerar el derecho al secreto de las comunicaciones y la obtención ilícita de pruebas.

En todo caso, una vez más, debe denunciarse la falta de una regulación legal completa de esta compleja materia, tan novedosa y cambiante por otra parte, por lo que la jurisprudencia tiene que llevar a cabo la siempre difícil y delicada tarea de complementar el ordenamiento jurídico (SSTS 630/2008, de 8 de octubre; 776/2008, de 18 de noviembre; 760/2008, de 26 de diciembre; ATS 811/2009, de 2 abril).

B. La obtención de los protocolos de Internet (IPS)

Las IPS son claves de acceso que los proveedores de servicios de Internet asignan a cada ordenador en el momento en el que se conecta a Internet. Su utilidad en la investigación penal se basa en que permiten identificar a través de dichos proveedores, el número telefónico desde el que se produce la conexión.

La jurisprudencia del Tribunal Supremo ha tenido ocasión de pronunciarse sobre la licitud de las búsquedas en Internet que realiza la Policía rastreando las redes de intercambio de archivos con el fin de averiguar la identidad de los usuarios que descarguen o comparten archivos de contenido delictivo, como por ejemplo los que contuviesen fotografías o vídeos de pornografía infantil.

Desde el principio, el Tribunal Supremo ha entendido que no es necesaria la previa autorización judicial para que la Policía pueda hacer este tipo de rastreos, dado que el acceso a dicha información puede efectuarla cualquier usuario. La huella de la entrada queda registrada siempre y esto lo sabe, o debiera saberlo, el propio usuario de la red que es quien la ha introducido.

Por tanto, no se precisa de autorización judicial para conseguir lo que es público. Se trata de datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes.

Con base en los fundamentos expuestos, entiende el Tribunal Supremo que estos datos no se encuentran protegidos ni por el art. 18.1, que reconoce el derecho a la intimidad, ni por el art. 18.3 CE que proclama el secreto de las comunicaciones (SSTS 236/2008; 292/2008, de 28 de mayo; 776/2008, de 18 de noviembre).

VELASCO NÚÑEZ[27] entiende que estas búsquedas en Internet constituyen *una inspección ocular del mundo virtual que no afecta a áreas de privacidad ni a secretos comunicativos, se hace exactamente igual que en el mundo convencional*.

Conviene subrayar que las IPS no identifican a una persona concreta, sino tan sólo un terminal informático. Por ello, cuando lo que se pretende es conocer el número de teléfono al que corresponde esa IP y su titular sí será necesaria autorización judicial, tal y como se desprende de la normativa reguladora de la protección de datos de carácter personal y de la legislación general sobre telecomunicaciones (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de 21 de diciembre 2007, que entró en vigor el 31 de marzo de 2008, y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y su Reglamento de 15 de abril de 2005).

De esta manera, parece claro que una vez averiguado el *Internet Protocol* de quien obtiene el material pedófilo, mediante el rastreo policial del espacio público, las subsiguientes actuaciones de identificación y localización de quien tiene asignado ese IP se deben llevar a cabo bajo control judicial.

La posición expuesta no resulta muy congruente con la regulación contenida en la Ley 25/2007 de Conservación de datos que exige para la cesión de estos datos a los funcionarios policiales, con carácter general, una autorización judicial previa, lo cual carece de sentido toda vez que se trata de acceder a un dato que el propio interesado ha permitido que sea de público conocimiento.

Por ello, el ámbito de aplicación de la citada disposición debe entenderse referida a los supuestos en los que para el progreso de las diligencias de investigación desarrolladas por las Fuerzas y Cuerpos Policiales en la persecución de actividades delictivas de cualquier naturaleza fuera necesario conocer el IP (o el número telefónico) de una determinada persona que hasta el momento es desconocido. En este caso resulta clara la necesidad de acatar esa exigencia legal.

A la vista de lo expuesto, dada la complejidad de la materia, su ductilidad, y las singulares características de la normativa que la regula, una vez mas será la jurisprudencia de nuestros tribunales la que tenga que ir perfilando un cuerpo de doctrina que atienda a las peculiaridades de cada caso en concreto.

---

[27] VELASCO NÚÑEZ, E., «Pericias informáticas: aspectos procesales penales», *Revista de Derecho,* núm. 4, 2009.

4. Valoración del deber de conservación en su transposición al ordenamiento español por la Ley 25/2007, de 18 de octubre

Los primeros problemas que se han planteado a propósito de la nueva de la Ley 25/2007, derivan de su rango normativo. Según algunos autores[28] debería haberse adoptado la forma de Ley Orgánica dado que su regulación puede afectar al contenido esencial de los derechos fundamentales a la intimidad y al derecho al secreto de las comunicaciones.

También la jurisprudencia del Tribunal Supremo se ha hecho eco de esta crítica, al declarar que, 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 (STS 249/2008, de 20 de mayo).

En las críticas expuestas subyace, una vez más, la tensión o equilibrio que debe inspirar el binomio o la dialéctica seguridad *versus* libertad. Esto es, eficacia sin merma de las garantías.

Asimismo, la doctrina ha puesto de manifiesto que el deber de retención tiene un carácter general, esto es, se funda en un mandato legal dirigido a los proveedores de forma generalizada, con independencia del supuesto de hecho concreto que en el futuro pueda fundamentar la obligación de cesión de dichos datos a instancia de la autoridad judicial. El deber de retención persigue, así, conservar unos datos que eventualmente pueden ser útiles en la investigación de una concreta infracción penal.

Se trata de conservar de forma generalizada sin individualizar ni los sujetos ni las comunicaciones concretas que pueden verse afectadas por la medida.

El carácter generalizado del deber de conservación de datos ha sido criticado en cuanto que no cumple con el principio de intervención indiciaria que exigen las medidas restrictivas de los derechos fundamentales orientadas a la prevención o persecución de los delitos[29]. Se apoya en el riesgo genérico de que se puedan cometer delitos para cuyo esclarecimiento puedan ser útiles los datos previamente conservados. Este riesgo es tan genérico que no justifica la legitimidad del deber de conservación generalizada impuesto por el legislador.

Ello no obstante, no han faltado autores[30] que han justificado el deber de conservación generalizada de los datos vinculados a las comunicaciones electrónicas al

---

[28] A juicio de Ortiz Navarro y Lucas Martín la Ley desarrolla de forma directa el contenido y régimen jurídico del derecho fundamental al secreto de las comunicaciones

[29] Martín Morales, *El principio constitucional de intervención indiciaria: test de alcoholemia, videovigilancia, cacheos, redadas y controles policiales, hallazgos casuales, intervenciones domiciliarias, telefónicas, penitenciarias, aduaneras y otras,* Grupo Editorial Universitario, Granada, 2000.

[30] Gerreiro Picó, *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal,* Thomson-Civitas, Navarra, 2006, pp. 464 y 465; Ruiz Miguel, C., «El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», *Revista de Derecho Comunitario Europeo,* num.14, enero abril 2003, p. 41.

entender que existen otros supuestos de intervención indiciaria constitucionalmente admitidos.

Pero no se puede olvidar que también en estos casos, como por ejemplo los registros en los aeropuertos o las videocámaras en los bancos, la falta de indicios concretos se compensa por las especiales circunstancias que concurren en el lugar que hacen razonable la intervención o control.

Según una parte de la doctrina[31] esta obligación tiene una finalidad preventiva de delitos ya que la conservación de los datos no esta destinada a la investigación criminal de modo directo sino indirecto, ya que se lleva a cabo antes de la comisión del hecho delictivo e incluso antes de la sospecha de que pueda cometerse en un período determinado. Por tanto, no se puede hablar de una finalidad procesal inmediata en cuanto se lleva a cabo al margen de actuaciones derivadas de una *notitia criminis.*

Por ella la doctrina sitúa este deber de conservación en el ámbito de las medidas prospectivas.

Hay que recordar que, no cabe decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos, toda vez que el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan en la mente de los encargados de la investigación penal, por muy legítima que sea esta aspiración, pues de otro modo se desvanecería la garantía constitucional (STC 49/1999).

El Tribunal Constitucional, como es bien sabido, ha cerrado el paso a las denominadas intervenciones prospectivas (STC 171/1999) o de prevención desligadas de la realización de un hecho delictivo. Se trata de una medida *post delictum*, dictada una vez que ha llegado al Juez la *notitia criminis* y, normalmente tras haber recaído el auto de incoación del sumario[32].

También desde un punto de vista técnico, los expertos[33] han criticado el ámbito subjetivo y objetivo de la Ley pues sólo se refiere a los datos generados por el acceso a Internet, la telefonía por Internet y el correo electrónico. Llaman la atención sobre el hecho de que siendo distinto un proveedor de Acceso de un Prestador de servicios, la Ley solo contempla como sujetos obligados a los primeros. Esta limitación tiene como consecuencia negativa que, precisamente, es en los proveedores de servicios donde se encuentran fundamentalmente los datos de tráfico que permiten iniciar las investigaciones.

También, esta nueva regulación ha recibido críticas de los internautas que consideran que la obligación legal impuesta podría traducirse en una pérdida de con-

---

[31] González López, J.J, «La retención de datos de trafico de las comunicaciones en la Unión Europea: una aproximación crítica», *Diario La Ley*, num. 6456, 5 de abril de 2006.

[32] Jiménez Campo, J., *La garantía constitucional del derecho al secreto de las comunicaciones, op. cit.,* p. 70.

[33] Salom Clonet, J., «Incidencia de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos», *op. cit.,* p. 148.

fianza en la confidencialidad de los datos. Los usuarios se sienten vigilados lo que puede afectar a su libertad de expresión e información. Además, los criminales conscientes de que los datos de las comunicaciones que se lleven a cabo quedarán registrados, adoptarán las precauciones necesarias para ocultar el rastro de la misma, por lo que su eficacia quedará reducida al ámbito de la pequeña criminalidad.

Otra importante crítica se refiere al gran coste que supone para los operadores de estos servicios que han de realizar las adaptaciones precisas para cumplir con sus obligaciones de conservación y cesión de datos. Las previsiones de la Ley exigen una enorme inversión para los sujetos obligados para almacenar y conservar los datos de los millones de comunicaciones que se producen a diario.

En todo caso, y a pesar de las consideraciones expuestas, no se puede negar la utilidad que los datos conservados pueden prestar en la investigación penal. Una mirada hacia atrás en la ejecución de las comunicaciones puede aportar mucha luz en el esclarecimiento de algunas actuaciones delictivas[34]. De hecho, a la vista del resultado de una intervención, el órgano judicial puede solicitar del operador los datos de las comunicaciones producidas con anterioridad.

Por todo ello, me gustaría terminar resaltando la necesidad de avanzar en el camino de la actualización y de la búsqueda de nuevas técnicas de investigación que abran nuevas posibilidades en la investigación criminal, como medio necesario para hacer frente a los nuevos desafíos de la criminalidad organizada en la red, siempre dentro del respeto al contenido esencial de los derechos fundamentales y a los principios básicos del Derecho Penal y del proceso debido.

RESUMEN: Las nuevas tecnologías de la información y de la comunicación han tenido una influencia decisiva en el proceso de globalización. La extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de comunicación y de transmisión de información a gran velocidad ha supuesto la superación de las formas tradicionales de comunicación.

Pero la facilidad de acceso y el carácter anónimo y descentralizado facilita la perpetración del delito y dificulta su persecución. Por ello, las técnicas basadas en el análisis de los datos vinculados a las comunicaciones electrónicas, han ido adquiriendo una importancia creciente, por su gran utilidad en la prevención, investigación y enjuiciamiento de delitos, en particular, en asuntos de especial gravedad como la delincuencia organizada y el terrorismo. Esta utilidad unida al hecho de que se trata de datos que se difuminan enseguida, han sido factores decisivos en el deber de conservación de estos datos que el legislador comunitario ha impuesto a las empresas de telecomunicaciones y servidoras de Internet.

Pero, el establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, debe efectuarse buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la inviolabilidad de de las comunicaciones. Resulta necesario ponderar despacio esta injerencia en la esfera de los derechos fundamentales, aun en el caso de que esté prevista en la Ley, para que

[34] Moreno Catena, V., «Ley de conservación de datos y garantías procesales», *op. cit.,* p. 165.

no se desvirtúe el contenido esencial de los derechos fundamentales afectados tal y como éstos se reconocen por los textos constitucionales e internacionales.

PALABRAS CLAVE: Comunicaciones electrónicas, telecomunicaciones, deber de conservación de datos, derecho al secreto de las comunicaciones, derecho a la intimidad, derecho a la protección de datos de carácter personal, delincuencia organizada, principio de proporcionalidad, juicio de necesidad**.**

ABSTRACT: The new technologies of information and Communications have had a decisive influence in the process of globalization. The extraordinary expansion of the telecommunication networks and, in particular, Internet as a high speed means of communication and transmission of information have overcome traditional means of communication.

But the simplicity of access and its decentralized and anonymous character facilitates the perpetration of new crimes and makes more difficult to persecute those crimes. Hence, the techniques that are based in the analysis of data linked to electronic communication have acquired a growing importance, as they are very useful in the prevention, investigation and persecution of crimes, in particular, in cases that are specially in serious cases as organized crime and terrorism. This usefulness, tied to the fact that these kind of data can be blurred easily, have been decisive factors in the duty to preserve them that has been imposed by the European legislator to the telecom companies and to the IP providers.

However, imposing this kind of obligations, which is justified in order to Project public security, must be done respecting the necessary balance with the respect to those individual rights that can be affected by it, such as those related to privacy and the inviolability of communications. It seems mandatory to carefully ponder this interference in the sphere of fundamental rights, even when it may come from a formal law, so as to make sure that the essential content of those fundamental rights is not affected, such as they are shaped by constitutional and international legal texts.

KEY WORDS: Electronic Communications, telecommunications, duty to preserve personal data, the right to secrecy in communications, right to privacy, right to obtain protection of data of a personal nature, organized crime, principle of proportionality, judgment of necessity.