Jesús Alberto Messía de la Cerda Ballesteros.

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LAS TELECOMUNICACIONES.

Jesús Alberto Messía de la Cerda Ballesteros.

LA PROTECCIÓN DE DATOS DE CARÇACTER PERSONAL EN LAS TELECOMUNICACIONES.

Universidad Rey Juan Carlos.

A mis padres.

INDICE

Introducción.

El desarrollo de las diversas actividades requiere como presupuesto necesario, dada su natural alteridad, la gestión de variada información personal. Los prestadores de bienes y servicios necesitan conocer las circunstancias personales de sus clientes para poder adecuar su oferta a las necesidades y deseos de aquéllos. La Administración no puede desarrollar correctamente sus funciones sin conocer de forma precisa quienes son los destinatarios. La asunción de las consecuencias de los actos exige determinar quienes son responsables de los mismos. En definitiva, es indiscutible la esencialidad de los datos de carácter personal para realizar de la forma más satisfactoria una actividad.

Esta observación no está exenta, sin embargo, de algún inconveniente. Concretamente, el tratamiento de los datos de carácter personal puede llevarse a cabo de una manera lesiva para los derechos de la persona. Este peligro se agrava si aquellas operaciones se llevan cabo a mediante el empleo de medios informáticos, dada la elevada capacidad de procesamiento de la información que poseen. Pues bien, la amenaza es todavía mayor cuando esos medios están conectados entre sí. Es decir, la lesión a los mencionados derechos puede tener mayor alcance cuando la información se produce, gestiona, procesa, almacena y transmite por medios de telecomunicación, principalmente medios telemáticos. Nos referimos, con esta terminología, a los diversos instrumentos, equipos, sistemas y demás de tipo informático que están conectados entre sí a través de las redes de telecomunicación. Rápidamente el lector entiende que a la capacidad de procesamiento mencionada se une las enormes posibilidades de flujo de la información a indeterminados puntos de destino.

La potencial agresividad de las telecomunicaciones respecto de la información personal alcanza grandes proporciones. Estas comunicaciones generan una serie de datos de carácter personal exclusivos de las mismas, cuyo tratamiento es presupuesto necesario del servicio prestado: datos de facturación y tráfico de las llamadas telefónicas, de navegación en el caso de Internet, además de los anteriores. Incluso propician, en algunos casos, la transmisión de los datos por motivos de interés general: interconexiones entre redes, llamadas a números de emergencia.

Por otra parte, el grado de sofisticación tecnológica alcanzado provoca que el tratamiento de los datos derivado de muchas de las comunicaciones efectuadas sea desconocido de gran parte de los usuarios: por ejemplo, el caso de las cookies en Internet y otros supuestos de tratamiento invisible, como vamos a ver. Internet es una red de telecomunicaciones que, como tal, participa en muchos aspectos de las características generales de las mismas. Sin embrago, también se debe reconocer que goza de unas connotaciones específicas, que exigen su tratamiento separado. A problemas como el de las cookies, ya mencionadas se unen los resultantes de la aparición de instrumentos de comunicación propios de este medio. Nos referimos, entre otros, al correo electrónico o a los foros de Internet. En algunos casos, tales

novedades han requerido la atención del legislador, lo cual exige un planteamiento concreto de dichas cuestiones.

Como se puede comprobar, Internet, como vehículo de telecomunicación, genera problemas inexistentes hasta su aparición. Por ello, resultará comprensible la estructura de este trabajo. En primer lugar, se abordan las cuestiones relativas a la protección de datos en las telecomunicaciones tradicionales, las telefónicas. En el Capítulo II se analizan la protección de los datos de carácter personal en relación con Internet. Tal esquema no implica que las soluciones sean diversas en ambos casos. Ello dependerá del problema en cuestión. Así, existen cuestiones cuya resolución es idéntica en los dos casos, con independencia de la naturaleza de la comunicación, y otras que, por su especificidad, obtiene una solución diferente.

Este trabajo tiene por objeto el análisis de la protección de datos de carácter personal en las telecomunicaciones. No obstante, existe otro bien jurídico que también puede resultar lesionado por el uso de aquéllas: nos referimos al secreto de las comunicaciones. No es nuestra pretensión desentrañar y solventar los numerosos problemas que este derecho fundamental plantea. Sin embargo, sí se debe tener en cuenta que es necesario analizar cuál es el ámbito de este derecho y del derecho a la protección de datos de carácter personal, con el fin de determinar el destino de la normativa que se estudia en este libro. De esta forma, es necesario averiguar, desde un inicio, cuál es la naturaleza jurídica de los datos de tráfico generados por las comunicaciones.

Sin pretender extenderos, es conveniente dejar constancia aquí de la gran perentoriedad de la normativa sobre esta materia. La velocidad de los avances en las tecnologías de la informática y las comunicaciones (TIC) es vertiginosa, por lo que no es de extrañar que el Derecho se encuentre algo retrasado en su regulación. No obstante, a la imposibilidad provocada por el rápido desarrollo, se debe unir la conveniencia de que el legislador goce de cierta perspectiva, de forma que evite, en la medida de lo posible, errores que exijan posterior rectificación.

Aunque la obra esta actualizada, es obvio que seguirán surgiendo novedades regulatorias sobre esta materia. En cualquier caso, ya es posible analizar, con perspectiva suficiente, los problemas de la protección de datos de carácter personal en este sector, con independencia de la evolución normativa. Este es el propósito de este trabajo.

LA PROTECCION DE DATOS DE CARACTER PERSONAL EN EL ÁMBITO DE LAS TELECOMUNICACIONES.

1. Introducción.

La prestación de diversos servicios por los operadores de telecomunicaciones a través de las redes de telecomunicaciones accesibles al público[1], en virtud de los contratos que previamente han celebrado aquéllos con los usuarios de dichos servicios, conlleva necesariamente la obligación en éstos últimos, como contrapartida, de proporcionar una serie de datos de carácter personal que permitan la identificación de quien procede a su uso y, por tanto, asume la obligación del pago de dichos servicios. Hasta aquí, no se aprecia ninguna particularidad que permita diferenciar el tratamiento jurídico de la protección de los datos de carácter personal en el sector de las telecomunicaciones. Como en cualquier supuesto de contratación, es necesario que las partes manifiesten de modo claro quienes son, para garantizar la correcta ejecución del contrato. La particularidad reside en el hecho de que, además de estos datos proporcionados en un momento previo a la prestación del servicio, durante esta fase posterior se generan una serie de datos identificativos de cada comunicación y los sujetos intervinientes.

Lógicamente, la utilización continua y variada de estos servicios requiere la determinación exacta de cada acto de comunicación que se efectúa, tanto en interés del operador como de la protección de los usuarios. En primer lugar, el operador necesita conocer de modo preciso cuáles y cuántas han sido las llamadas efectuadas por un usuario, su duración y demás información que le permita ejercer su derecho de cobro correctamente y con éxito. Por otra parte, tal determinación del uso del servicio es una consecuencia necesaria del derecho de los consumidores y usuarios a una información transparente y precisa sobre el uso que han hecho de aquél como forma de proteger su posición débil, frente a la imposibilidad de tal pretensión en el caso contrario de opacidad. No se puede negar que la facturación detallada que recibimos en nuestros hogares nos dota de un medio defensa frente a los posibles abusos de los operadores, dado que nos permite concretar la reclamación sobre cobro indebido, a la vez que favorece el control en el uso de los medios telefónicos.

Sin embargo, tal beneficio no aparece solo en los modos actuales de facturación, sino que va acompañado de un potencial peligro. Como dijimos anteriormente, las empresas del sector de telecomunicaciones no sólo recaban datos con ocasión de la celebración de un contrato para la obtención de bienes o servicios. Además, cada acto de comunicación genera una serie de datos de carácter personal. Tal generación se produce en el tiempo en el mismo momento en que el usuario efectúa la llamada o comunicación: los datos se crean a la vez que se llama. Pues bien,

[1] Operador de servicios de telecomunicaciones y red pública de comunicaciones electrónicas son conceptos técnicos definidos por la legislación sobre telecomunicaciones, como tendremos ocasión de ver en páginas posteriores.

la aparente simplicidad de tal afirmación esconde, sin embargo, un problema de calificación jurídica. En efecto, la simultaneidad de la generación y captación de datos por una parte y el desarrollo de la comunicación por otra, plantean la posibilidad de que, en realidad, primero y segunda sean una manifestación de la misma realidad y que, por tanto, requieren el mismo tratamiento y protección jurídicos. En definitiva, se discute si los datos generados por la comunicación forman parte de la misma, junto con su contenido, o por el contrario reflejan una realidad distinta que debe ser protegida por normas diferentes a las relativas al secreto de las comunicaciones.

2. La naturaleza jurídica de los datos de facturación y tráfico.

La primera cuestión que se plantea en el análisis de esta categoría de datos es la relativa a la determinación del significado de los términos empleados. Concretamente, debemos estudiar si las palabras facturación y tráfico hacen alusión a la misma realidad o, por el contrario, se refieren a datos diferentes. Tal cuestión tiene importancia, en cuanto que los regímenes jurídicos pueden ser también diferentes. Para ello, resulta conveniente analizar la regulación española y los antecedentes comunitarios.

El artículo 65 del Real Decreto 1736/1998, de 31 de Julio, que aprueba el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones[2], acoge la regulación sobre los datos de facturación y tráfico, como se deduce de su encabezado y se cita expresamente más adelante. Concretamente, su párrafo 1º establece la obligación de destrucción de los datos de los usuarios y abonados[3]

---

[2] Como señala Loza Corera, resulta criticable la adopción de una norma de rango reglamentario para regular la protección de los datos de carácter personal en el sector de las telecomunicaciones. Máxime, cuando el precepto central de la misma establece una remisión, a su vez, a la normativa general, tanto comunitaria como de derecho interno. LOZA CORERA, MARIA. *Nueva legislación europea de protección de datos*. Diario la Ley, núm. 5549. Año XXIII. 22 de Mayo de 2002. Pág. 4. Pues bien, esta normativa no ha sido derogada por la Ley 32/2003, de 3 de Noviembre, general de Telecomunicaciones.

[3] En relación con la alusión conjunta a los usuarios y los abonados respecto de los datos de tráfico y facturación, encontramos algunas deficiencias, a nuestro modo de ver. Tanto la legislación interna como la comunitaria definen los usuarios como aquella persona que utiliza un servicio público de telecomunicaciones, aunque no haya contratado el servicio, según establece la segunda. Se entiende por abonado la persona que es parte en el contrato con el proveedor del servicio para la prestación del mismo. Ante tales definiciones, entendemos que los datos de identificación que se captan a raíz de una comunicación sólo pueden ser los relativos a los abonados, pues en realidad éstos se identifican como consecuencia de la utilización de su terminal. La determinación de quien sea la persona que, en cada acto de comunicación, efectúa una llamada desde un terminal concreto, no se deduce del acto de la llamada en sí, con lo cual no debería poder captarse, en tanto que no es dato de tráfico en sí y tampoco se requiere para la posterior facturación del servicio. Es decir, los datos sobre los usuarios no son parte del acto de la comunicación en sí. Cuando una de las partes en la conversación dice "hola, soy Juan", está ya en el seno de la comunicación misma, por lo que tal

almacenados por el establecimiento de la llamada, mientras que el párrafo 2º admite la posibilidad de tratar los datos almacenados previamente por motivos de facturación y limitar la cantidad de datos que se pueden tratar de entre los recogidos. Es esta una solución idéntica a la acogida en el artículo 6 de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de Diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la Intimidad en el sector de las telecomunicaciones, derogada por la Directiva 2002/58/CE, de 12 de julio de 2002, del Parlamento europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[4].

En realidad, parece que se trata, por tanto, de una sola categoría de datos, que se distingue tan solo por la necesidad posterior de satisfacer una fin, el de la facturación. Los datos recogidos y luego utilizados con tal objetivo son, en sí mismos, idénticos. La única diferencia radica en el volumen de los datos que, en principio, se recogen con ocasión de la comunicación y los que posteriormente se pueden conservar para realizar las tareas de facturación y cobro, que son inferiores a los primeros, según se deduce del artículo 65 del Reglamento, que reproduce el Anexo de la antigua Directiva 97/66.

El anterior argumento se reforzaba en la Propuesta de reforma de la Directiva 2002/58, en la cual se equipara la regulación sobre el tratamiento de los datos de tráfico y de facturación. Aunque efectivamente la categoría de los datos agrupados bajo ambas denominaciones sea prácticamente idéntica, sin embargo no estamos seguros de que la solución acogida en la Propuesta fuera la más satisfactoria para los intereses de los afectados. En dicho texto, la asimilación consistía en la posibilidad de que los datos de tráfico puedan conservarse para fines de promoción comercial y para la prestación de servicios de valor añadido. Es decir, se acogía

---

información no forma parte de los datos generados por el tráfico, sino que son parte del propio objeto del tráfico. Tal argumentación se justifica en mayor medida si tenemos en cuenta que la normativa establece la prohibición de conservación como regla general, dado que tal rigurosidad está en más consonancia con la protección reforzada del secreto de las comunicaciones, que con el régimen de protección de datos. De todas formas, en páginas posteriores analizamos detenidamente la naturaleza de los datos de tráfico y facturación.
Idéntica solución sostenemos para los datos de los abonados obtenidos por el tráfico, como vamos a ver a continuación, pues la mera participación en un contrato por los abonados no puede condicionar el nivel de protección de sus datos respecto de los usuarios.
Por estas razones, no entendemos que ambas regulaciones aludan a los datos del usuario en relación con los datos de tráfico. La identificación de aquél no forma parte, por supuesto, de los datos que se pueden conservar con fines de facturación, pues aquélla excede de los fines perseguidos en ésta. Ahora bien, tampoco comprendemos qué necesidad puede existir de conocer los datos de quien es el sujeto que efectivamente llama para lograr el establecimiento de llamada, fin confesado por la norma para la recogida de estos datos.

[4] DOCE de 31 de Julio de 2002. L 201/37. http//:www.europa.eu.int.

respecto de aquéllos el régimen que la Directiva 97/66 establecía respecto de los datos de facturación.

Aunque estas cuestiones se tratan en líneas posteriores, ya adelantamos nuestras dudas respecto de esta ampliación de las posibilidades de los operadores y, por tanto, la restricción de los derechos de los afectados. No es, a nuestro modo de ver, la naturaleza de los datos el criterio que legitima la diferente regulación de los mismos, sino más bien la finalidad a la que se destinan los mismos. En este sentido, la conservación de los datos de facturación se justifica por razones de cumplimiento efectivo de la relación jurídica existente, circunstancia que no concurre en los datos de tráfico una vez concluida la comunicación. De ahí, que no se justifique adecuadamente esta solución. La Directiva 2002/58/CE parte de la necesidad de dotar a los operadores de unas posibilidades que eviten la estrechez del régimen de la Directiva 97/66 y que proporcionen una posición más adecuada a las circunstancias actuales de competencia en el mercado. Es decir, una vez más priman criterios de naturaleza económica.

Corripio Gil-Delgado sostiene la separación de ambos tipos de datos. Para ello, se apoyaba en las redacciones contenidas en la Propuesta de reforma de la Directiva 97/66, en virtud de la cual son datos de tráfico aquellos tratados *en el curso de la transmisión de una comunicación o necesario para garantizar esta transmisión*. Respecto de los datos de facturación, señala la Propuesta que *podrán ser tratados los datos sobre tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones.* Como señala la autora, la redacción de este segundo precepto ya apuntaba la distinción propuesta, pues la remisión a aquellos datos que sean *necesarios*, implica que no todos pueden ser tratados por motivos de facturación[5]. En definitiva, los diferentes objetivos que se pretenden satisfacer con cada uno de aquéllos impide, en cumplimiento del principio de finalidad, la equiparación. Aunque la definición de los datos de tráfico ha sufrido alguna alteración en el texto final, sin embargo el artículo 6.2 de la Directiva 2002/58/CE permite mantener el mismo criterio.

En un sentido similar se pronuncia De Asís Roig, para quien los datos de tráfico se requieren como presupuesto del acto de comunicación, en tanto que son necesarios para llevar a cabo su encaminamiento, mientras que los datos de facturación se exigen para satisfacer una consecuencia de la comunicación, cual es su cobro[6]. Se observa así una clara diferencia de los fines que cada tipo de información satisface. En este sentido parece abundar el Considerando 15 de la Directiva

---

[5] CORRIPIO GIL-DELGADO, MARIA DE LOS REYES y MARROIG POL, LORENZO. *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones.* Agencia de protección de datos. MADRID, 2001. Págs. 187-191.

[6] DE ASIS ROIG, AGUSTÍN E. *Protección de datos y derecho de las telecomunicaciones.* En *Régimen jurídico de Internet.* Colección derecho de las telecomunicaciones (coordinadores: Javier Cremades, Miguel Angel Fernández-Ordóñez y Rafael Illescas). Ed. La Ley. MADRID, 2002. Pág. 219.

2002/58/CE, según el cual se consideran datos de tráfico los relativos al encaminamiento, duración o la hora de la comunicación efectuada.

En relación con lo anterior, Cervera Navas[7] plantea sus dudas respecto de la solución del consentimiento tácito para el tratamiento de estos datos con fines comerciales y la prestación de servicios de valor añadido, puesto que la información que se proporciona para posibilitar aquél es, en la mayoría de los casos, escueta y se presenta de forma no muy clara, como cláusula adjunta a la factura. Por eso, sostiene que la Propuesta ampliaba la información que se debe facilitar en estos casos: concretamente, se exigía información sobre el tipo de datos que se va a tratar y la finalidad del tratamiento. A este respecto, no entendemos que la inclusión de un precepto en tal sentido implique un aumento de las garantías y protección de los afectados, puesto que tales exigencias se deducen de la Directiva 95/46, que, como norma de regulación general, resulta de aplicación igualmente en el sector de las telecomunicaciones en lo que no se halle expresamente regulado en la Directiva sectorial. Quizás por lo anterior, el artículo 6.4 de la Directiva 2002/58 no exige información sobre la finalidad del tratamiento e incluye, como novedad, dicho deber respecto de la duración del tratamiento. Además, como señala Cervera, sería conveniente que se determine qué es servicio de valor añadido, con el fin de evitar que tal concepto se infle con supuestos que no se corresponden con el mismo y evitar el régimen más riguroso de los mismos.

Por otra parte, el planteamiento de la cuestión relativa a la naturaleza jurídica de los datos de tráfico y facturación no sólo presenta interés desde un punto de vista estrictamente teórico, sino que además tiene una consecuencia práctica importante. La configuración de los datos de facturación como datos de carácter personal o como parte del mensaje, del contenido de la comunicación, implica que o bien su régimen jurídico se acoge en la legislación de protección de datos o, por el contrario se trata de una cuestión que encaja en la regulación que protege el secreto de las comunicaciones. Si se adoptara la primera solución sería admisible la cesión de los datos de facturación al Ministerio Fiscal, según determina el artículo 11.2 de la LOPD, sin necesidad de autorización alguna. En cambio, si se entendiera que se trata de una parte en sí del contenido de la comunicación, entonces el acceso al mismo requeriría autorización judicial, según se deduce del artículo 18.3 de la CE.

Ambas opciones han sido defendidas. En efecto, con ocasión de un proceso judicial la Fiscalía General del Estado defendió el carácter indisoluble del proceso de comunicación, con todos sus componentes, a lo que se contestó en sentido contrario, defendiendo la separación en el tratamiento jurídico de algunos elementos de aquélla. Vamos a situar ambas posiciones.

---

[7] CERVERA NAVAS, LEONARDO. *Comentarios a la Propuesta de reforma de la Directiva 97/66 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.* Jornadas sobre Protección de la Privacidad, Telecomunicaciones e Internet. Pamplona, 2000. Pág. 3.

Esta polémica se inició como consecuencia de un proceso en el que se juzgaba el acceso indebido a los equipos de una empresa de sistemas informáticos por parte de personas que actúan de forma anónima, con el fin de borrar algunos ficheros. El Ministerio Fiscal solicitó a la compañía telefónica la información relativa al acto de comunicación en cuestión, a lo que ésta respondió que no puede facilitar la misma sin una autorización judicial. Ante tal negativa, la Fiscalía de procedencia eleva consulta a la Fiscalía General del Estado. Es la consulta 1/99[8]. En la misma se sostenía que los datos de facturación debían considerarse datos de carácter personal, por lo que debía admitirse su cesión al Fiscal sin necesidad de intervención judicial.

Sin embargo, no fue esta la solución adoptada por el órgano consultado. En primer lugar, manifestó la indisolubilidad de los elementos de los diferentes elementos de la comunicación, por lo que se concluyó afirmando la extensión material u objetiva del secreto de las comunicaciones a los datos de facturación. Además, se sostiene que la protección que brinda el secreto de las comunicaciones se extiende temporalmente más allá del tiempo en que ésta se produce: no sólo se protege en tiempo real, sino también en momentos posteriores.

También se esgrimía un argumento de técnica legislativa. Se entendía que la ubicación de estos datos en la normativa de protección, pues la legislación de telecomunicaciones y de servicio postal distingue entre interceptación de contenido y acceso a los datos del tráfico, no es sino un error, pues los preceptos de la legislación de telecomunicaciones y de servicio postal no pueden configurar el contenido esencial de un derecho fundamental por su naturaleza ordinaria, tarea que corresponde exclusivamente a la propia Constitución y al Tribunal Constitucional. Finalmente, sostenía el carácter sensible de este tipo de datos y la posibilidad de que los mismos puedan recibir un grado de protección superior al establecido por la legislación de protección de datos en aplicación del principio de protección más amplia, dado que en esta materia los precedentes comunitarios y del Consejo de Europa establecen una regulación de mínimos.

Frente a esta posición, Ancos Franco[9] considera que es necesario hacer una calificación jurídica diversa del contenido de la comunicación y de los datos identificadores para su facturación. Aunque se reconoce que el contenido del mensaje no puede disociarse del proceso de comunicación en sí, sin embargo sí se justifica un tratamiento jurídico diverso. Para esta autora el medio y momento en el que se generan los datos de facturación no puede implicar la aplicación de regímenes jurídicos diferentes a los datos de carácter personal. Sólo sería admisible tal diferencia

---

[8] *Consulta 1/99*. LA LEY. Diario núm. 4734, de 15 de Febrero de 1999.

[9] ANCOS FRANCO, HELENA. *El tratamiento automatizado de los datos personales en el ámbito de las telecomunicaciones. Comentario a la Consulta 1/99 de la Fiscalía General del Estado.* LA LEY. Diario núm. 4812, de 7 de Junio de 1999. Pág. 2036.

normativa según el soporte físico en el que se contienen los datos: la normativa de 1982 sobre Intimidad se aplicaría a la información contenida en soporte papel, mientras que la información automatizada sería objeto de regulación por la legislación de protección de datos[10].

Continúa la autora afirmando que los datos de facturación gozan de entidad propia, que los diferencia de otros elementos de la comunicación: se trata de información decisiva para el cobro del servicio y de gran interés comercial, lo que para aquélla los acerca al sentido dinámico que de los mismos se recoge en la legislación sobre protección de datos. Además, sostiene que tales datos encajan perfectamente en tal regulación, pues los mismos pueden revelar rasgos definitorios del sujeto. Apoyándose en las alegaciones de la Fiscalía consultante, Ancos afirma la diferencia de régimen normativo y, por tanto, de protección que se deduce de la ubicación de los datos de facturación en los preceptos de las normativas sectoriales relativos a la protección de datos de modo expreso. Más decisiva resultaba, a juicio de la autora, la Directiva 97/66, relativa al tratamiento de datos personales en el sector de las telecomunicaciones, que incluye en su ámbito objetivo los datos de facturación, a la vez que se remite, en lo no regulado expresamente, a la Directiva 95/46, que recoge el régimen general de protección de datos. Frente a la argumentación de la Fiscalía General del Estado sobre las deficiencias normativas de las legislaciones sectoriales, sostiene la autora que las conclusiones de aquélla son contrarias a criterios elementales de interpretación, pues restringe, sin razón alguna para ello, el sentido del artículo 50 de la antigua Ley General de Telecomunicaciones, mientras que interpreta de modo extensivo el siguiente artículo, dedicado al establecimiento de prohibiciones. A continuación analizaremos estos preceptos. Concluye la autora negando el carácter sensible de los datos de facturación que sostiene la Fiscalía General del Estado, pues se trata de una categoría que la legislación de protección de datos acoge de modo taxativo.

Al igual que Ancos Franco, la Agencia Española de Protección de Datos opta por la solución de encuadrar los datos de facturación dentro del ámbito de aplicación de la protección de datos de carácter personal. En repetidas ocasiones, la autoridad de control ha señalado que la cesión de tales datos al Ministerio Fiscal por parte de empresas, cualquiera que sea su actividad, debe someterse a las previsiones establecidas en el artículo 11.2 d) que, exonera del consentimiento del afectado parda llevar a cabo aquéllas, sin necesidad de concurra ningún otro requisito[11]. La respuesta de la Agencia Española de Protección de Datos no se plantea el problema de la naturaleza de los datos de tráfico y facturación, pues da por entendido que se trata de datos de carácter personal. En alguna de aquéllas, la Agencia aludía a la cesión de datos de carácter personal, sin expresa mención de que se tratase de datos de

[10] Si se observa la fecha del artículo citado, se comprenden las distinciones de regulación según el soporte que las contiene, pues la LORTAD comprendía en su ámbito exclusivamente los datos automatizados. A la luz de la Ley de 1999, ya no se puede sostener tal tesis.

[11] Tal posición se deduce, por ejemplo, de las Memorias de la Agencia Española de Protección de Datos de 1998 y 1999.

facturación telefónica, sino a datos en general de aquella naturaleza, ante los términos generales de dichas consultas. Sobre esta base, no se puede entender que la respuesta de la Agencia sea adecuada al caso presente, por la particular idiosincrasia de los datos de facturación y tráfico.

El Consejo de Europa también parece concebir los datos de tráfico y facturación como datos de carácter personal en sentido estricto, sometidos, por tanto, a la normativa sobre protección de los mismos. La Recomendación R (95) 4, adoptada por el Comité de Ministros el 7 de febrero de 1995, sobre la protección de datos de carácter personal en el ámbito de los servicios de telecomunicaciones, estableció en el punto 3.1 de su Anexo que la recogida y tratamiento de los datos de carácter personal sólo podrá hacerse, entre otras, por razones de facturación, aplicando a continuación toda una serie de preceptos propios de la protección de datos. Sin embargo, el punto 2 del Anexo prohibía, salvo excepciones, toda injerencia en el contenido de la comunicación, por entender que se trata de una violación de la vida privada, el secreto de la correspondencia y la libertad de las comunicaciones.

La adopción de una postura a este respecto no resulta fácil, si tenemos en cuenta que ambas partes de la discusión utilizan argumentos loables y defendibles, al menos a priori, a la vez que algunas incorrecciones. Efectivamente, los datos de facturación gozan de un carácter claramente personal. Sin embargo, tampoco se puede negar la idea de que tales datos y el proceso de comunicación en sí parecen indisolubles, de modo que su representación intelectual no se presenta de forma separada. En cualquier caso, resulta conveniente analizar si la generación de los datos en el momento de la comunicación implica alguna especialidad que pueda justificar su diferencia de tratamiento jurídico.

En principio, no cabe duda que las diferentes realidades contenidas en el acto de comunicación pudieren ser separadas, como de hecho así ocurre. Efectivamente, los datos de facturación, una vez concluido el acto de comunicación, sobreviven en el tiempo. Estos datos se incluyen automáticamente en un fichero destinado a la determinación exacta del coste del servicio correspondiente a cada llamada. Tal inclusión es una excepción a la prohibición de recogida y tratamiento de los datos generados en la comunicación sin el consentimiento del afectado. Efectivamente, el artículo 65[12], párrafos 1 y 2, del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, establece que

> *1. Los operadores deberán destruir los datos de carácter personal sobre el tráfico relacionados con los usuarios y los abonados que hayan sido tratados y almacenados para establecer una comunicación, en cuanto termine la misma, sin perjuicio de lo dispuesto en los apartados siguientes.*

[12] Este precepto, como ya se ha señalado, desarrollaba el artículo 6 de la Directiva 97/66/CE del Parlamento europeo y del Consejo, de 15 de Diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

> *2. Podrán ser tratados por los operadores, exclusivamente con objeto de realizar la facturación, y los pagos de las interconexiones, los datos a los que se refiere el apartado anterior que incluyan:*
> *a) el número o la identificación del abonado.*
> *b) La dirección del abonado y el tipo de equipo terminal empleado para las llamadas.*
> *c) El número total de unidades que deben facturarse durante el ejercicio contable.*
> *d) El número de abonado que recibe la llamada.*
> *e) El tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitidos.*
> *f) La fecha de la llamada o del servicio.*
> *g) Otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes.*
> *Estos datos podrán tratarse y almacenarse únicamente por el plazo durante el cual pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable. Transcurrido dicho plazo, los operadores deberán destruir los datos de carácter personal, en los términos del apartado 1 de este artículo.*

Como se puede deducir de la parte final del apartado 2º, se trata de datos exclusivamente destinados a la determinación del coste de las llamadas, tanto desde el punto de vista del usuario, que podrá reclamar cobros indebidos y devoluciones sobre la base de los mismos, como del operador, que tendrá un fundamento preciso para la exigencia del precio. De ahí que, aún estableciendo esta excepción a la prohibición del tratamiento de estos datos, tal autorización no vaya más allá de la satisfacción de los fines perseguidos y, en consecuencia, concluye cuando ya no pueden o deben satisfacerse sus fines, el pago o la reclamación de los usuarios o abonados. Claro está que en el supuesto de que se inicie un procedimiento con motivo del pago de la factura, dichos datos podrán conservarse durante el tiempo que duren los mismos, al destinarse aquéllos precisamente a la determinación de la cantidad adeudada, que es el fin de estos datos[13]. Por lo demás, el precepto analizado es, sencillamente, una manifestación del principio de finalidad de los datos contenido en el artículo 4 de la LOPD, cuyo párrafo 5º establece que

---

[13] A este respecto, la Agencia Española de Protección de Datos, al igual que la Comisión del Mercado de las Telecomunicaciones, permite la conservación durante el plazo de tres meses para impugnar la factura, según el artículo 31 del Reglamento del Servicio Universal, y durante el plazo de cinco años que se otorga al operador para reclamar el pago de la factura si fuera impagada y estuviese vencida, según el artículo 1966 del C.C. AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 2000*. Pág. 404.

> *5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados*[14].

La exigencia del cumplimiento de finalidad del artículo 4 no admite, han señalado algunos autores, la concepción de la lista de datos recogida en el artículo 65.2 del RSU, como un *numerus apertus*[15]. El estricto cumplimiento de los fines no permite ampliar en exceso dicho listado, de forma que el mismo puede considerarse como una manifestación de dicho principio de finalidad.

Podrían plantearse dudas respecto de la necesidad de conservar todos los datos mencionados, respecto de la proporción entre el volumen de datos tratados y almacenados y su necesidad para los fines perseguidos. Por ejemplo, el dato relativo al abonado que recibe la llamada. Si la determinación del coste se realiza, entre otros factores, atendiendo a la zona (local, provincial, interprovincial, extranjero) del destino de llamada, parece que sería suficiente con determinar la misma, sin necesidad de precisar el destinatario específico. En cualquier caso, se trata de cuestiones que exceden de los objetivos perseguidos en este trabajo. Tan sólo pretendíamos ubicar el problema.

Como se ha podido observar, la separación de los datos de facturación respecto del resto de los elementos de la comunicación es una realidad. Tal posibilidad de tratamiento posterior es contraria, por tanto, a la concepción del acto de comunicación como una realidad indisoluble. Ahora bien, tal posibilidad fáctica no necesariamente debe llevarnos a sostener sin mayor detenimiento la consecuencia de una separación del régimen jurídico aplicable. Es cierto también que, desde un punto de visto objetivo o material, los datos de facturación encajan sin problemas en la definición que la legislación de protección de datos contiene sobre los datos de carácter personal. En efecto, dicha información está referida a una persona identificada o identificable. A la vista de todo lo anterior, existen poderosos argumentos para sostener que tales datos deben regularse por la legislación de protección de datos, de manera que la cesión de los mismos al Ministerio Fiscal se puede realizar sin necesidad de intervención judicial ni de consentimiento del afectado.

Sin embargo, no resulta del todo claro que las características externas al núcleo de la comunicación, a su contenido, no formen parte del bien jurídico protegido en este caso. El carácter personal de estos datos no tiene por que ser la única nota distintiva de los mismos a los efectos de la determinación de su régimen jurídico. Sin negar que efectivamente aquéllos permiten la identificación de un sujeto,

---

[14] Este artículo reproduce el artículo 6.1 e) de la Directiva 95/46.

[15] En tal sentido se han manifestado CARRASCO PERERA, ANGEL, MENDOZA LOSANA, ANA I. e IGARTUA ARREGUI, FERNANDO. *Comentarios a la Ley general de telecomunicaciones.* ARPON DE MENDIVIL ALDAMA, ALMUDENA y CARRASCO PERERA, ANGEL (Directores). Ed. Aranzadi. PAMPLONA, 1999. Pág. 685.

sin embargo no resulta tan claro que igualmente no constituyan parte integrante de la comunicación en sí. En tal sentido, entendemos que, a diferencia de lo que sostiene Ancos respecto de la nula importancia del momento de generación de los datos, considerando que el factor determinante para realizar la calificación jurídica es el soporte o continente de los datos, el factor temporal sí puede ayudar a despejar dudas y realizar dicha calificación de modo apropiado, como se deduce de la posición de la Fiscalía General del Estado. No en vano, una de las especialidades que justifica la existencia de una legislación sectorial de las telecomunicaciones sobre protección de datos es precisamente la automaticidad y velocidad de sus procesos, lo cual exige el establecimiento de una serie de garantías técnicas adicionales a las previsiones de la legislación general sobre protección de datos. Así se deduce de varios Considerandos de la Directiva 2002/58. Sin ánimo de excedernos en esta cuestión, el Considerando 5º, por ejemplo, de esta Directiva, señala lo siguiente:

> *Actualmente se están introduciendo en las redes públicas de comunicación de la Comunidad nuevas tecnologías digitales avanzadas que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios. El desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de comunicaciones electrónicas. El acceso a las redes móviles digitales está ya disponible y resulta asequible para un público muy amplio. Estas redes digitales poseen gran capacidad y muchas posibilidades en materia de tratamiento de los datos personales. El éxito del desarrollo transfronterizo de estos servicios depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad.*

Cuando analizamos una comunicación observamos que la misma se compone de un contenido, el mensaje transmitido, y de un continente, el proceso de la comunicación en sí, como recuerda la Fiscalía. Pues bien, según la doctrina del Tribunal Constitucional, el secreto de las comunicaciones comprende tanto la primera como los datos atinentes al segundo[16]. En definitiva, no sólo se protege el objeto de la

---

[16] Efectivamente, el Tribunal Constitucional ha recogido esta doctrina en la sentencia 114/84, de 29 de Septiembre, a la cual se alude en la Resolución de la Consulta 1/99 por la Fiscalía General del Estado. Preferimos reproducir aquí un fragmento de la citada sentencia, por su esclarecedora redacción: *"…El bien constitucionalmente protegido es así - a través de la imposición a todos del "secreto" – la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje – con conocimiento o no del mismo -, o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo). Por ello, no resulta aceptable lo sostenido por el Abogado del Estado en sus alegaciones en el sentido de que el artículo 18.3 de la CE protege sólo el proceso de comunicación y no el mensaje, en el caso de que éste se materialice en algún objeto físico. Y puede también decirse que el concepto de "secreto", que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales. La muy reciente sentencia de 2 de Agosto de 1984 del Tribunal Europeo de Derechos del Hombre – caso Malone – reconoce expresamente la posibilidad de que el artículo 8 de la Convención pueda resultar violado por el empleo de un artificio técnico que,*

comunicación, sino ésta misma, de manera que el alto Tribunal considera que tal secreto no sólo se vulnera por el conocimiento del mensaje, sino más aún, por el conocimiento de que se ha establecido una comunicación. Se deduce, así, la importancia del factor temporal en la determinación de la naturaleza de los datos de facturación, pues su generación en tiempo real supone necesariamente que se trata de datos identificativos de la comunicación que se realiza: no podría referirse a una comunicación concreta si no se generasen en el preciso instante de ésta, pues en un momento posterior no se puede ya saber cuál ha sido su duración exacta, el destinatario u otros datos.

En definitiva, estos datos se generan en tiempo real porque, en realidad, describen las características específicas de cada comunicación, es decir, porque, además de su naturaleza de datos de carácter personal, son también datos relativos al proceso o acto de comunicación. Parece, por tanto, que sobre la base del ámbito de protección del derecho fundamental al secreto de las comunicaciones, señalado por el Tribunal Constitucional, los datos de facturación y tráfico encajan en dicho derecho. Sin negar, por tanto, el carácter personal de estos datos, lo cierto es que parecen gozar de una naturaleza mixta. La configuración como elemento integrante del secreto de las comunicaciones de los datos de tráfico y facturación se justifica si tenemos en cuenta que la libertad de entablar aquéllas se puede ver afectada, no sólo por el hecho de conocer su contenido, sino también el hecho mismo de la comunicación: en muchas ocasiones resulta suficiente tener la posibilidad de saber que se puede producir o que se ha producido la comunicación para condicionar a los sujetos que participan de éstas, de manera que se limita su libertad de actuación.

Esta posición ya había sido defendida en nuestro país por la doctrina. A juicio de Martín Morales, entre otros, el artículo 18.3 protege todo el proceso de comunicación, no sólo su contenido. De esta forma, el registro de datos relativos a los actos de comunicación requiere, o bien consentimiento de los interesados o bien autorización judicial. Es decir, se protegen a través del artículo 18.3 los datos relativos a la comunicación en sí misma[17]. En el mismo sentido se pronuncian Roca Junyent y Torralba Mendiola[18], al incluir en el ámbito de protección del secreto de las

---

como el llamado "comptage", permite registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma". BOE de 21 de Diciembre de 1984. Bases de datos de jurisprudencia de EL DERECHO.
Más adelante volveremos sobre el estudio de esta resolución, pues de la misma se deducen otros aspectos relevantes para determinar la naturaleza de los datos de facturación.

[17] MARTIN MORALES, RICARDO. *El régimen constitucional del secreto de las comunicaciones.* Ed. Civitas. MADRID, 1995. Págs. 56-57.

[18] ROCA JUNYENT, MIGUEL y TORRALBA MENDIOLA, ELISA. *Derecho a la intimidad: el secreto de las comunicaciones e Internet.* En *Régimen jurídico de Internet.* Colección Derecho de las telecomunicaciones (Coord. CREMADES, JAVIER; FERNANDEZ-ORDONEZ, MIGUEL ANGEL; ILLESCAS, RAFAEL). Ed. La Ley. MADRID, 2002. Pág. 195.

comunicaciones, no sólo el hecho mismo de la comunicación, sino también circunstancias externas de ésta, como por ejemplo la identidad de las partes.

No obstante todo lo anterior, no resulta fácil adivinar ya en este momento, cual puede ser la solución del problema. Por el contrario, existen otros argumentos que pueden inclinar al intérprete en sentido inverso. A la luz de la sentencia del Tribunal Constitucional 114/84, se podría llegar a la conclusión de que los datos de tráfico y facturación encajan en el ámbito de protección que proporciona el derecho fundamental al secreto de las comunicaciones, de forma más correcta que en el propio de la protección de datos de carácter personal. Sin embargo, pudiere ocurrir entonces que, según la doctrina esgrimida por el Tribunal Constitucional en la mencionada sentencia, la consecuencia práctica fuera precisamente un menor grado de protección para los datos de carácter personal que no se generen durante la comunicación para fines de facturación. Por las propias circunstancias del caso planteado, la Fiscalía General del Estado no se planteó tal posibilidad, pues se estaba debatiendo sobre la cesión de datos a un tercero, sin entrar a analizar las facultades de los intervinientes en la comunicación respecto de otro tipo de datos no contemplados en este caso. Sin perjuicio del interés que despierta tal supuesto, dejamos su estudio para una pregunta posterior. Sin embargo, en relación con la doctrina del Tribunal Constitucional, debemos hacer una precisión.

Si los datos de carácter personal que se manifiestan en la comunicación se encuadran en el ámbito del artículo 18.4 y no del artículo 18.3, podría entenderse lo mismo respecto de los datos de tráfico y facturación, pues la información que se deduce de éstos puede ser idéntica a la que contienen aquéllos. No obstante, a pesar de que el contenido de ambas informaciones pudiera asimilarse, dado el carácter personal de las mismas, no parece que dicha asimilación de soluciones resulte válida. Cuando el Tribunal Constitucional alude a la información íntima o nosotros estudiamos los datos de carácter personal de la comunicación, en realidad se hace referencia a información personal recogida en su contenido, en el mensaje. Sin embargo, en el caso de los datos de facturación no se está tratando sobre dicho contenido. La sentencia 114/84 excluye del ámbito del secreto de las comunicaciones aquello que *en la conversación telefónica* pueda entenderse como concerniente a su vida privada, sin que excluya de aquél la información generada *a causa de la comunicación*. En efecto, afirma la citada sentencia que

> *"…quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica una aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera "íntima" del interlocutor, pudieren constituir atentados al derecho garantizado en el artículo 18.1 CE".*
> En líneas posteriores se lee lo siguiente: *"Si se impusiera un genérico deber de secreto a cada uno de los interlocutores o de los corresponsales "ex" artículo 18.3, se terminaría vaciando de sentido, en buena parte de su alcance normativo a la protección de la esfera íntima personal "ex" artículo 18.1,*

> *garantía ésta que, "a contrario", no universaliza el deber de secreto, permitiendo reconocerlo sólo al objeto de preservar dicha intimidad".*

Sensu contrario, puede entenderse que tanto el contenido no íntimo como la información relativa a la comunicación en sí, que no forma parte de la conversación, quedan dentro de tal ámbito. Además, resulta bastante obvio que la argumentación de la sentencia respecto de la posibilidad de difusión del contenido de una comunicación, no es válida para los datos de facturación, pues los mismos no se conocen por las partes. No puede ser de otra manera, pues tales datos no van inicialmente destinados a las partes (aunque después tenga derecho a conocerlos por la factura), sino al operador que facilita su conexión y que actúa como tercero. En realidad, la protección de los datos de facturación debe existir frente a terceros, en concreto, frente al operador telefónico, sin que preocupe tanto la protección de tales datos entre las personas que participan en la llamada.

Por otra parte, aunque los datos de facturación informan sobre determinados aspectos de la actividad de las personas, sin embargo prevalece en los mismos su configuración como información relativa a la comunicación. Aunque pueda servir para otros fines ulteriores, su objetivo inmediato es determinar la cuantía del precio del servicio: la información de facturación define y delimita la comunicación. Si no se pudiese recabar, sencillamente no se conocería como ha sido aquélla, por lo que difícilmente se podría exigir el pago, dado el carácter ilíquido de la deuda. No negamos que efectivamente los datos de facturación especifiquen circunstancias de inequívoco carácter personal, lo cual resulta lógico si tenemos en cuenta que la determinación de la deuda exige, por supuesto, conocer la persona a quien se pretende solicitar el pago. Quizás por ello, tales datos gozan de una naturaleza híbrida. No obstante, como en cualquier otra deuda, las precisiones que sobre los elementos personales se realizan persiguen la configuración de la obligación, se obtienen en razón de la misma y no tienen como fin directo y exclusivo la identificación personal. Así, tales datos superan su evidente índole subjetiva, para referirse de modo inmediato a la configuración de los actos de comunicación.

Por estas razones, el artículo 65 del RSU exige la necesidad del consentimiento del afectado para tratar los datos de facturación con fines comerciales, como establece con carácter general la LOPD para tratar datos de carácter personal, mientras que guarda silencio respecto de tal requisito cuando los datos se destinan a su fin propio. Es decir, parece que su utilización para el fin inicial les excluye de la solución que la normativa de protección de datos de carácter personal establece para los mismos. En efecto, tras admitir sin mayor requerimiento el tratamiento y almacenamiento de estos datos para el citado fin, el párrafo 3º del artículo 65 establece que

> *3. Asimismo, los operadores podrán tratarlos datos a los que se refiere el apartado anterior para la promoción comercial de sus propios servicios de telecomunicaciones, siempre y cuando el abonado haya dado su consentimiento*

> *previo. A estos efectos, los operadores deberán dirigirse a los abonados, al menos, con un mes de antelación al inicio de la promoción, requiriendo su consentimiento que, de producirse, será válido hasta que los abonados lo dejen sin efecto de modo expreso. Si en el plazo de un mes desde que el abonado reciba la solicitud, éste no se hubiere pronunciado al efecto, se entenderá que consiente, sin perjuicio de lo dispuesto en la disposición transitoria séptima.*

Todas estas razones inducen a pensar que tal información no es equiparable a aquella otra de naturaleza personal que se contiene en la comunicación, ni mucho menos de los datos de carácter personal que los prestadores de servicios de comunicación tienen de sus usuarios por razón de la relación existente entre ambos. Más bien, como información del proceso de comunicación en sí mismo, su régimen jurídico sería el propio del secreto de las comunicaciones.

Existen otros argumentos que apoyan la postura mantenida por la Fiscalía General del Estado. Según Ancos Franco[19], los preceptos contenidos en las disposiciones reguladoras de los servicios de telecomunicaciones y de servicio postal universal permiten afirmar con rotundidad la distinción entre regímenes jurídicos diversos para el secreto de las comunicaciones y la protección de datos de carácter personal, a la vez que con la misma claridad se observa que los datos de facturación encajan en el supuesto de hecho regulado por los artículos referentes a la segunda. Pues bien, no apreciamos tal claridad en la exposición normativa y sí vemos posibilidades de una argumentación contraria a la realizada por esta autora.

Respecto de la legislación del sector de las telecomunicaciones, la Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones, contiene una serie de preceptos Capítulo III, relativos al secreto de las comunicaciones y a la protección de datos personales. Nos referimos a los artículos 33 y siguientes. Establece el primero de ellos lo siguiente:

> *Los operadores que exploten redes públicas de comunicaciones electrónicas 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.*
>
> *Asimismo, los operadores deberán adoptar a su costa las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de Mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.*

---

[19] ANCOS FRANCO, HELENA. *Op. cit.* Pág. 2038.

Por su parte, el artículo 34, que encabeza con la leyenda relativa a la protección de datos de carácter personal, dispone que

> *Sin perjuicio de lo previsto en el apartado 6 del artículo 4 y en el segundo párrafo del artículo anterior, así como en la restante normativa específica aplicable, los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público o deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal, conforme a la legislación vigente.*
>
> *Los operadores a los que se refiere el párrafo anterior deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta ley en esta materia*[20]*. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.*

Como se puede observar, la redacción de los dos preceptos es prácticamente idéntica en lo relativo a la exigencia de deberes de garantía y a los sujetos sometidos a los mismos. Tan sólo existe una diferencia, pues en el artículo 34 se añade la expresión *en el ejercicio de su actividad*, que no figura en el artículo 33. En principio, tal apostilla no parece hacer referencia alguna que permita adivinar en el citado artículo un sentido diferente al que recoge el artículo 33. Sin embargo, también se puede pensar que la utilización de tal expresión no es gratuita, de manera que algo se pretende expresar con la misma. Para Ancos, la utilización de tales términos es congruente con la configuración de los datos de facturación como datos de carácter personal, pues entiende que son datos generados en el ejercicio de su actividad, que es la prestación de los servicios de telecomunicaciones. A nuestro entender, tal interpretación pudiera resultar un tanto forzada. En realidad, el precepto sólo establece la necesidad de que se protejan los datos de carácter personal con ocasión de las actuaciones propias de los operadores, no que los datos de carácter personal deban ser generados en aquellas actuaciones. Si así fuera, los datos proporcionados por los particulares al contratar el servicio no quedarían encuadrados en tal régimen de protección, pues los mismos existen con anterioridad al establecimiento de la relación entre ambas partes.

En nuestra opinión, tal frase hace alusión a las obligaciones que, respecto de la protección de los datos de carácter personal, competen a los operadores de servicios y redes de telecomunicaciones en todas sus actuaciones en relación con los

---

[20] Sobre medidas de seguridad de los ficheros que contienen datos de carácter personal, *vid.* Real Decreto 994/1999, de 11 de Junio.

mismos. Es decir, todos los actos llevados a cabo por aquéllos relativos a dichos datos, como su recogida, tratamiento, facturación, etc., deben someterse a las previsiones de la legislación de 1999. Ahora bien, la información que genera la comunicación se rige por lo dispuesto en el artículo 33. Los datos a los que se refiere el artículo 34 son los proporcionados por los afectados y que son necesarios para los distintos actos de los operadores, pero no todos aquéllos que aparezcan como consecuencia directa de la llamada realizada, máxime si tenemos en cuenta la interpretación que el Tribunal Constitucional ha realizado respecto del ámbito objetivo del secreto de las comunicaciones, como ya se vio anteriormente. La actividad de los operadores de telecomunicaciones, a que se refiere el artículo 34, no hace referencia, como no puede ser de otra manera y en ningún caso, a su participación en los actos de comunicación. De ahí que falte tal expresión en el artículo 33, relativo a la información que se encuadra en el secreto de las comunicaciones. Así, podríamos afirmar que los datos del artículo 34 son los obtenidos por los operadores cuando ellos son parte directa, es decir, cuando reclaman los datos de los particulares para prestar el servicio, pero no se incluyen los generados como consecuencia de una relación entre terceros que aparecen y se manifiestan en la comunicación.

En consonancia con lo anterior, no podemos estar de acuerdo con las afirmaciones que la autora citada hace respecto de lo que, a su juicio, es una interpretación restrictiva del artículo 34 (y antiguo artículo 50 de la Ley 11/1998, de 24 de Abril, general de Telecomunicaciones) por parte de la Fiscalía General del Estado. En realidad, la inclusión de los datos de facturación en el ámbito de aplicación del artículo 33, no minimiza el alcance de los datos de carácter personal, sino que más bien determina su correcto sentido. Por todas las razones expuestas, los primeros son parte esencial e inseparable de la comunicación en sí, aún su posible referencia a información de naturaleza personal.

Por la misma razón antes apuntada, también debemos rechazar la idea de que la Consulta 1/99 interpreta de modo extensivo el artículo 51 (en la nueva ley, artículo 35), cuando en realidad se trata de un precepto restrictivo. En este caso, discutimos que su naturaleza sea efectivamente restrictiva. Según el artículo,

> *Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de tareas de control para la eficaz utilización del dominio público radioeléctrico establecidas en el Convenio internacional de telecomunicaciones, sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:*
>
> *a) La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.*

> *b) Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos.*
>
> *Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de telecomunicaciones.*
>
> *Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye en artículo 61.2* (artículo 43.2 de la Ley 32/2003).

Pues bien, no se trata de restringir derechos, que sería el factor que imposibilitaría la extensión del ámbito del precepto más allá de los expresamente recogidos en el mismo. Por el contrario, se establece una restricción sí, pero de las posibles actuaciones de los poderes públicos, con el fin de mantener la extensión de los derechos de los particulares, concretamente la libertad de sus comunicaciones. Es decir, en realidad se trata, no de aminorar la protección de los derechos sobre los que versa esta regulación, sino de todo lo contrario, evitar la presión vulneradora de los mismos.

Señala Ancos que el artículo 51 al que nos estamos refiriendo, hace referencia exclusiva a los contenidos de las comunicaciones. Efectivamente, la redacción de dicho artículo alude expresamente a los contenidos de las comunicaciones en las letras a) y b) del apartado 1º. Sin embargo, si tal mención se entiende en sentido estricto, entonces se puede sostener como conclusión que la Administración puede conocer, por motivos de control datos de facturación derivados de esas comunicaciones, sin que tenga la obligación de destruirlos, pudiendo almacenarlos y sin que tenga que adoptar medidas que eviten el riesgo de interceptación. Claro está, parece que tal conclusión no puede sostenerse, por su falta de lógica. Para evitar tan absurda interpretación, creemos que podría entenderse el término contenido como sinónimo de todo aquello que forma parte de la comunicación, por lo que los datos de facturación formarían parte del mismo.

Efectivamente, existen otros pasajes de la normativa sobre servicios de telecomunicaciones que, en principio, no admiten otra conclusión que la configuración de los datos de facturación como datos de carácter personal. Por ejemplo, la leyenda del artículo 65 del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones se refiere a los datos personales de facturación. Ahora bien, frente a este criterio de interpretación sistemático, nunca hemos negado que la información facilitada por este tipo de datos también goza de un claro carácter personal. Sin embargo, esto no es suficiente para someter los mismos a la regulación de protección de datos. Dicho de otro modo, los datos de tráfico y facturación son datos de naturaleza personal que forman parte del contenido de las comunicaciones, lo cual justifica la adopción del régimen jurídico propio de éstas.

Quizás si pueda ser más definitivo en este sentido el párrafo 5º del artículo 65. Según el mismo,

> *A los efectos de lo dispuesto en este artículo, de conformidad con el artículo 3 de la Ley de Regulación del Tratamiento Automatizado de Datos de Carácter Personal* (hoy, la LOPD)*, se entiende por tratamiento de datos el conjunto de operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación conservación, elaboración, modificación, bloqueo, cancelación y cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*

Como se puede observar, este precepto reproduce lo dispuesto en el artículo 3 de la LOPD respeto de la definición de tratamiento de datos. Su colocación dentro del artículo 65 puede inducirnos a sostener, por un elemental criterio sistemático de interpretación, que toda la regulación contenida en tal artículo hace referencia a los datos de carácter personal. Ahora bien, la corrección en la ubicación de los preceptos y la utilización de conceptos no es precisamente la mayor en la legislación sobre comunicaciones.

Grandes dudas y deficiencias respecto de la determinación del contenido del secreto de las comunicaciones y de la protección de datos personales se plantean a la luz de la legislación sobre servicios postales. Frente a lo que algunos pudieren pensar, tal normativa no es proverbialmente clara respecto de la determinación de la naturaleza de los datos de carácter personal. En principio, la Ley 24/1998, de 13 de Julio, de Regulación del Servicio Postal Universal y de Liberalización de los Servicios Postales, recoge en su artículo 3, relativo al secreto e intervención de las comunicaciones postales, dos párrafos, cada uno de los cuales alude a diferentes conceptos. Señala este precepto que

> *1. En la prestación de los servicios postales, los operadores deberán garantizar el secreto de las comunicaciones, de conformidad con el artículo 18.3 de la Constitución, y el cumplimiento de lo establecido en el artículo 55.2 de ésta y en el artículo 579 de la Ley de Enjuiciamiento Criminal.*
>
> 2. *Los operadores que presten servicios postales no podrán facilitar ningún dato relativo a la existencia del envío postal, a su clase, a sus circunstancias exteriores, a la identidad del remitente y del destinatario ni a sus direcciones. Se aplicará, en su caso, lo previsto en la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.*

Por una parte, el párrafo 1º, al aludir al secreto de las comunicaciones, parece referirse a la protección del contenido de éstas. Por otra, el párrafo 2º se remite a la LOPD para la protección de los datos relativos al envío postal, clase, circunstancias exteriores, identidad de remitente y destinatario y sus direcciones. Pues

bien, no estamos de acuerdo con el ámbito de protección que, según este precepto, se otorga a la legislación de protección de datos. Si parece claro que la misma tiene por objeto los datos de carácter personal, no entendemos qué razón puede justificar que también se encuadre en la misma información sobre la existencia del envío postal, su clase y sus circunstancias exteriores. No hay duda que se trata de características propias de la comunicación en sí, si no sobre su contenido, sí sobre su forma o vehículo. En definitiva, datos sobre la comunicación. Como ya se ha visto anteriormente, el contenido esencial del derecho al secreto de las comunicaciones se compone no sólo del contenido del mensaje o comunicación, sino también del hecho del mensaje en sí mismo. Por lo tanto, creemos que la legislación postal no sirve como argumento definitivo para la discriminación de los diferentes ámbitos de los derechos en cuestión. Si avanzamos en el análisis normativo, descubrimos que tal desorden se hace más palpable cuando consultamos la normativa reglamentaria o de desarrollo. El artículo 5 del Real Decreto 1829/1999, de 3 de Diciembre, por el que se aprobó el Reglamento por el que se regula la prestación de los servicios postales, en desarrollo de la Ley 24/1998, dispone lo siguiente:

> *1. Los operadores postales garantizarán el pleno respeto al secreto e inviolabilidad de las comunicaciones postales, la obligación de protección de datos y el cumplimiento de los requisitos establecidos por la normativa sectorial sobre seguridad del funcionamiento de la red en materia de transporte de sustancias peligrosas, protección del medio ambiente y ordenación territorial.*
>
> *2. Los operadores postales, en el ejercicio de las actividades de prestación de los servicios, garantizarán:*
>
> *a) El secreto e inviolabilidad de las comunicaciones postales, salvo resolución judicial, en los términos establecidos en los artículos 6 y 7 del presente Reglamento.*
>
> *b) El respeto al Honor, a la intimidad familiar y personal de los usuarios y el pleno ejercicio de sus derechos, en especial cuando el operador postal aplique técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias.*
>
> *c) La neutralidad y confidencialidad de los servicios postales.*
>
> *d) La igualdad de trato a los usuarios de los servicios postales que estén en condiciones análogas.*
>
> *e) La ausencia de cualquier tipo de discriminación, especialmente la derivada de consideraciones políticas, religiosas o ideológicas.*

Como se puede observar, el artículo 5 del Reglamento reconoce de forma separada, al igual que inicialmente hacía la Ley, el secreto de las comunicaciones y la protección de datos. Sin embargo, la concepción que de cada uno de éstos tiene esta norma no encaja con la regulación legal. El artículo 6.1 del Reglamento establece

> *1. El secreto de los envíos postales afecta al contenido de los mismos e implica la absoluta prohibición para los operadores postales y para sus*

> *empleados de facilitar dato alguno relativo a la existencia del envío postal, a su clase, a sus circunstancias exteriores, a la identidad del remitente y del destinatario o a sus direcciones, salvo petición de éstos, sus representantes legales o apoderados o mediante resolución judicial.*
>
> *En ningún caso podrán considerarse amparados por el secreto de las comunicaciones los contenedores, de cualquier naturaleza, que sirvan para transporte de los envíos postales.*

Como se puede ver con claridad, este precepto no es conforme con el artículo 3 de la Ley 24/1998, pues en el mismo solamente se hace referencia a la obligación de secreto y no a la protección de los datos de carácter personal, a la cual sí se refiere el precepto legal. Tal obligación de secreto, por la naturaleza de la información que se incluye en el mismo, no puede hacer referencia a otro tipo de secreto que no sea el de las comunicaciones. No obstante, existe otra circunstancia más importante si cabe: en el artículo 6 del Reglamento se incluyen, dentro del ámbito y protección del secreto de las comunicaciones, datos como la identidad de las partes del envío o sus direcciones. Es decir, se incluyen expresamente datos de naturaleza personal en el régimen del artículo 18.3, como parte integrante de la comunicación.

A continuación el párrafo 3º del artículo 6 reconduce, sin embargo, a la legislación de protección de datos, en el siguiente sentido:

> *2. El tratamiento de los datos de carácter personal contenidos en cualquier documento con soporte físico o electrónico, derivado de la prestación de los servicios postales por sus operadores, se someterá a las previsiones contenidas en la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de datos de Carácter Personal.*
>
> *La obligación de protección de datos incluirá el deber de secreto de los de carácter personal, la confidencialidad de la información transmitida o almacenada y la protección de la intimidad.*

Si se analiza con detenimiento este artículo, se observa que el tratamiento los datos de carácter personal a que se alude en el mismo es el *derivado de la prestación de servicios postales*, es decir, se hace referencia exclusiva a los datos previamente obtenidos como consecuencia de la relación entre operador y usuario por razón de la prestación de aquellos servicios. Tal expresión excluye, por tanto, cualquier posibilidad de considerar incluidos en este supuesto los datos recogidos en el envío y necesarios para realizar el mismo. Por lo tanto, tal información va unida al acto de la comunicación, de manera que se diferencian ambas categorías de datos a los efectos de la determinación de su régimen jurídico.

La confusión que introduce esta normativa alcanza cotas insospechadas en la última parte del párrafo 3º del artículo 6. Se establece que la protección de datos incluye el deber de secreto de los datos personales, la confidencialidad de la información transmitida o almacenada y la protección de la Intimidad. Como se puede

observar, se afecta al régimen jurídico de la protección de datos de carácter personal materias que pudieren versar sobre el secreto de la comunicación, concretamente el segundo tipo. La única justificación a esta solución, que sin embargo no dejaría de ser una incorrección, sería la consideración de la obligación de protección de datos en sentido amplio, más allá de los datos de carácter personal. Pero claro está, tal interpretación no sirve entonces a los propósitos de quienes sostienen el carácter exclusivamente personal de los datos de facturación.

En definitiva, lo que queremos reseñar es la inconveniencia de utilizar argumentos normativos, en concreto buscar apoyo en la legislación postal, para determinar la naturaleza de los datos de carácter personal, pues, como hemos visto, se trata de una regulación que adolece de rigurosidad en alguno de los conceptos jurídicos empleados.

Tampoco entendemos que la legislación comunitaria favorezca claramente la consideración como datos de carácter personal de los datos de facturación. En efecto, la Directiva 2002/58 establece una regulación sobre tratamiento de datos personales en relación con la prestación de servicios públicos de comunicaciones electrónicas, según se deduce del artículo 3 de la misma e, incluso, de su propio título. En el mismo sentido, se recoge normativa sobre los datos de facturación y tráfico en el artículo 6. Tales circunstancias podrían, en principio, servir para afirmar la consideración inicial. Ahora bien, la utilización del criterio sistemático de interpretación está justificada cuando el resultado de la misma no sea contrario al que proporcionan los conceptos empleados por la norma. Aunque la Directiva delimita el ámbito de la protección de datos de carácter personal en las telecomunicaciones, sin embargo la misma también reconoce, sin entrar en su regulación, la existencia de otros derechos y su alcance. El artículo 6 de la Directiva establece que

> *1. Sin perjuicio de lo dispuesto en los apartados 2,3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.*
>
> *2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.*
>
> *3. El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo*

necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento.

4. El proveedor del servicio deberá informar al abonado o al usuario de los tipos de datos de tráfico que son tratados y de la duración de este tratamiento a los efectos mencionados en el apartado 2 y, antes de obtener el consentimiento, a los efectos contemplados en el apartado 3.

5. Sólo podrán encargarse del tratamiento de datos de tráfico, de conformidad con los apartados 1,2,3 y 4, las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor añadido, y autorizadas de comunicaciones y de los datos de tráfico asociados a ellas cuando se lleven a cabo en el marco de una práctica comercial lícita con el fin de aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial.

6. Los apartados 1,2,3 y 5 se aplicarán sin perjuicio de la posibilidad de que los organismos competentes sean informados de los datos de tráfico con arreglo a la legislación aplicable, con vistas a resolver litigios, en particular los relativos a la interconexión o a la facturación.

Se observa que el tratamiento que la Directiva 2002/58 da a los datos de tráfico no se compagina con la regla sobre tratamiento de datos de carácter personal, pues exige la inmediata destrucción de los mismos, una vez que la comunicación ha concluido. Podría afirmarse que tal solución se adopta, en realidad, porque, siendo su captación necesaria para el establecimiento de la comunicación, no se justifica su conservación inconsentida por motivos que no sean los de facturación. Sin embargo, la Directiva señala que tal rigor se impone porque se trata de defender un bien jurídico distinto. Señala el Considerando 26 de la Directiva lo siguiente:

Considerando que los datos relativos a los abonados utilizados para el establecimiento de llamadas contienen información sobre la vida privada de las personas físicas y atañen a su derecho de respeto a la correspondencia,…

Es decir, no se trata sólo de defender la información de naturaleza personal vertida en la comunicación, sino que además se debe proteger *el respeto a su correspondencia*. No encontramos otra significación a la expresión respeto a la

correspondencia que la propia del secreto de las comunicaciones. Con tal mención se hace alusión a tal secreto, es decir, a la protección del contenido de la comunicación, en el cual incluye la Directiva los datos de tráfico y facturación. A lo anterior, debemos añadir que, como ya se ha señalado, se trata de una normativa de mínimos. De esta forma, nada obstaría a que las regulaciones internas de cada Estado impusiera mayores condiciones al tratamiento y cesión de los datos, entre los de facturación y tráfico.

La calificación de los datos de facturación y tráfico como elemento integrante del secreto de las comunicaciones ha sido la solución adoptada igualmente por los organismos comunitarios en varias ocasiones. En primer lugar, podemos citar la Recomendación 2/99 del Grupo de Protección de las Personas por lo que respecta al Tratamiento de Datos Personales (creado por la Directiva 95/46/CE, al amaro del artículo 29), adoptada el 3 de Mayo de 1999, sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones[21]. En dicha recomendación, el Grupo de Trabajo afirma lo siguiente:

> *El ámbito de aplicación de la presente recomendación contempla las interceptaciones en sentido amplio, es decir, la interceptación del contenido de las telecomunicaciones, pero también los datos correspondientes a las telecomunicaciones, y, en particular, posibles medidas preparatorias (tales como el "monitoring" o el "data mining" de los datos de tráfico) que se pudieran prever con el fin de decidir la oportunidad de la interceptación del contenido de la telecomunicación.*

Pues bien, el Grupo de Trabajo sostiene, en correspondencia con tales afirmaciones, que la interceptación de las telecomunicaciones constituye una violación del derecho a la Intimidad de las personas y al *secreto de la correspondencia.* En páginas posteriores, se define en la citada Recomendación el concepto de interceptación como

> *El conocimiento de una tercera parte del contenido y/o de los datos asociados a las telecomunicaciones privadas entre dos o varios corresponsales, en particular los datos de tráfico vinculados a la utilización de los servicios de telecomunicación*

---

[21] El Texto de esta Recomendación ha sido extraído de la página en Internet de la Unión Europea. Concretamente, www.europa.eu.int/comm/internal_market/
La cuestión de la interceptación de las comunicaciones por las autoridades competentes es también objeto de preocupación para el Gobierno español. En este sentido, desde hace algún tiempo los Ministerios de Fomento, Interior y Defensa están trabajando de forma conjunta para la elaboración de una normativa sobre esta materia. Esta normativa incluiría una serie de requisitos: en primer lugar, de carácter técnico (características técnicas de las comunicaciones entre los operadores y las autoridades competentes) y en segundo, requisitos materiales (tiempo de mantenimiento de la información por los operadores, tipo de información que se puede conservar). Como se puede observar, se observa en el ejecutivo español intenciones similares a las que otros Gobiernos ya han materializado. La importancia de esta cuestión, radica, como se analiza en otra parte del trabajo, en el régimen de las interceptaciones y, por ende, en las garantías proporcionadas a los usuarios.

En una nota a pie de página núm. 3 de la Recomendación, se afirma expresamente que

> *Este carácter amplio del concepto de interceptación de las telecomunicaciones corresponde al ámbito de aplicación de la Resolución del Consejo de 17 de Enero de 1995 relativa a la interceptación legal de las telecomunicaciones, ya citada, y al marco general de las disposiciones jurídicas aplicables sobre este tema...*

Como se puede observar, tal posición amplia no es sencillamente la propuesta de un órgano de consulta y examen del organigrama comunitario, sino que ha sido consagrada normativamente. La Resolución del Consejo de 17 de Enero 1995[22], relativa a la interceptación de las telecomunicaciones, como señala el Grupo de Trabajo en su Recomendación, aborda cuestiones puramente técnicas, sin detenerse en el análisis jurídico de aquéllas. Sin embargo, sí resulta de interés en cuanto reitera la posición amplia en la concepción de las interceptaciones. Entre los requisitos que las autoridades necesitan para efectuar las interceptaciones, se encuentra la posibilidad de acceso a distintos datos de la conexión, a saber: señal de entrada, número del abonado a quien se dirige la llamada, incluso si no llega a producirse la comunicación; número del abonado que realiza la llamada; señales producidas; inicio, fin y duración de la llamada; número conectado y otros posibles, si ha habido desvío de llamada; situación geográfica cuando la llamada se efectúa desde un teléfono móvil. Además, se añade la posibilidad de acceder a otras informaciones, como los servicios utilizados, las comunicaciones en tiempo real y demás que se citan en la Resolución. Ante todo lo anterior, parece que no existe ninguna duda de que la Resolución del Consejo contempla un concepto amplio de interceptación de las telecomunicaciones, lo que implica igualmente la concepción en el mismo sentido de éstas últimas, pues cuando se hace referencia a la interceptación de las comunicaciones se está aludiendo al ámbito del derecho fundamental al secreto de las comunicaciones, no a la regulación sobre protección de datos.

Todavía mayor claridad al respecto aporta la Directiva 2002/58, en su artículo 5, relativo a la confidencialidad de las comunicaciones, al establecer lo siguiente:

> *1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público…*

---

[22] Diario Oficial C329, de 14 de Noviembre de 1996. También se puede obtener en la página citada. *Vid. nota anterior.*

En relación con la Propuesta de Directiva, el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, emitió el dictamen 7/2000, de 2 de Noviembre (la reseña se cita en notas posteriores). La Propuesta de Directiva definía los datos sobre tráfico como *cualquier dato tratado en el curso de o a efectos de la transmisión de una comunicación a través de una red de comunicaciones electrónicas*[23]. A la vista de tal definición, el Grupo de Trabajo entiende que

> *La definición incluye asimismo los datos sobre localización generados durante la transmisión de una comunicación y los datos de navegación (como los URL o localizadores unificados de recursos), que pueden revelar intereses personales de los particulares (por ejemplo, sitios web que pueden ofrecer indicaciones sobre las creencias religiosas, las ideas políticas, la salud o la vida sexual de quienes lo frecuentan). Al indicar las páginas de un sitio web que han sido visitadas, revelan el contenido exacto al que ha podido acceder una particular.*
>
> *Puesto que los datos sobre tráfico pueden incluir este tipo de información personal, deberían estar revestidos de la confidencialidad prevista para las comunicaciones (artículo 5 y siguientes).*

Aunque efectivamente en el caso de comunicaciones a través de Internet, el acceso a los datos sobre los sitios o páginas a los que se ha navegado supone claramente el acceso al contenido de la comunicación, sin embargo en el supuesto de comunicaciones por voz (conmutación de circuitos, a diferencia de la comunicación en Internet, que se basa en un sistema de conmutación de paquetes) el conocimiento de datos sobre la llamada efectuada también permite conocer parte del contenido de la conversación en muchos casos, sin poder olvidar que, en muchas ocasiones, es el hecho de la llamada el que revela el dato de mayor importancia. De ahí que la definición recogida en la Propuesta y reproducida por el Dictamen (así como en la Directiva 2002/58/CE, según se ha visto) no distinga entre unos u otros tipos de datos sobre tráfico y que la solución jurídica propuesta en el segundo sea idéntica para todos ellos. Como se puede observar, la evolución tecnológica hace que las tendencias normativas avancen hacia el reconocimiento expreso de la concepción amplia del secreto de las comunicaciones y de la interceptación de las mismas. Hemos de tener en cuenta que existen muchas ocasiones en la que el sujeto que comunica no desea que se conozca, no ya el contenido de la conversación, sino incluso con quien se comunica, desde qué teléfono lo hace, etc., cuyo conocimiento podría coartar la libertad del sujeto en el establecimiento de aquéllas.

---

[23] Tal definición únicamente difiere de la definitiva de la Directiva 2002/58, en aspecto formal, pues define ésta, en su artículo 2 b), los datos de tráfico como *cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma.* Si bien de esta definición se pudiera deducir la equiparación de los datos de tráfico y facturación, sin embargo la limitación de la extensión de los segundos, según el artículo 6, permite mantener la separación la citada separación conceptual.

En otro orden de cosas, no estamos de acuerdo con la afirmación realizada por la Fiscalía general del Estado, en el sentido de que los datos de facturación son datos sensibles. No ponemos en duda la intención de la Fiscalía, que pretende justificar de nuevo, la conveniencia de un régimen de protección reforzado para los datos de facturación. En efecto, la Fiscalía señala que toda intromisión en la información íntima de una persona requiere previsión legal e intervención judicial, lo cual no es conforme con la posibilidad de cesión de los datos al Ministerio Fiscal sin necesidad de ningún otro requisito, como se deduce del artículo 11.2 d) de la LOPD. Sin embargo, no pensamos que el objetivo de la protección reforzada se pueda conseguir con el uso de tal argumento. Sin duda, la Fiscalía utiliza el adjetivo sensible en un sentido amplio que exprese la especialidad de tal información. No obstante, hemos de tener en cuenta, como señala Ancos, que se trata de una terminología acuñada por una legislación específica, la de protección de datos. La Ley de 1992, reproducida en este caso por la 1999, crean un tipo legal, en el que se encuadran un grupo determinado de datos de carácter personal y al que, en razón de su vinculación al ámbito íntimo de la persona, se dota de un régimen de protección reforzado.

Por lo tanto, el carácter taxativo del listado de datos incluidos en este concepto y la limitación de posibilidades de tratamiento de los mismos, imposibilita la realización de una interpretación amplia que permita la consideración como datos sensibles de aquéllos no mencionados expresamente por la Ley. Además, tal argumento conlleva la contradicción de que, siendo así, se podría reconducir la cuestión, siquiera indirectamente, al campo de los datos de carácter personal, lo cual no es precisamente el fin perseguido.

Antes de abandonar el análisis del problema de los datos de facturación, debemos abordar otro aspecto del mismo. La posible utilización de estos datos no sólo se lleva a cabo por el Ministerio Fiscal en sus actividades procesales, sino que además e incluso de modo más generalizado, sirven como un eficaz instrumento de investigación a las Fuerzas y Cuerpos de seguridad del Estado.

La Agencia Española de Protección de Datos ha recibido en repetidas ocasiones consultas de empresas relativas al modo de proceder de las mismas ante las solicitudes por parte de dichas Fuerzas, en el ejercicio de las funciones de Policía judicial, de los datos de facturación. Concretamente, la Agencia Española de Protección de Datos se refiere a los supuestos en los requerimientos de tal información no se ha apoyado en una autorización judicial o intervención en similar sentido del Ministerio Fiscal[24]. La respuesta de la Agencia en estos casos ha sido positiva, pues entiende que se trata de un supuesto de cesión que encaja perfectamente en los artículos 22 y 11.2 d) de la LOPD. El primero de los preceptos citados establece lo siguiente:

[24] Memoria de La Agencia Española de Protección de Datos de 1999.

Ficheros de las Fuerzas y Cuerpos de Seguridad

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

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

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Así, se admite la captación y tratamiento de datos sin consentimiento de los afectados, siempre que concurra alguno de los presupuestos habilitantes: que sean necesarios para prevenir un peligro real y grave para la seguridad pública, reprimir infracciones penales y que sean necesarios para los fines de una investigación concreta, cuando se trate de datos especialmente protegidos, debiendo ser cancelados cuando desaparezcan las circunstancias que motivaron la recogida y tratamiento. Además, se exige que la solicitud sea precisa, específica para cada caso y motivada. Argumenta también, a mayor abundamiento, que la obligación de notificar de forma inmediata los datos recogidos y tratados al Juez y al Ministerio Fiscal, según el artículo 445.1 de la LOPJ, permite subsumir tal supuesto en el precepto contenido en el artículo 11.2 d), según el cual no se requiere consentimiento del afectado para la cesión de datos cuando ésta tenga por destinatarios, entre otros, a los Jueces y Tribunales y al Ministerio Fiscal.

La posición adoptada por la Agencia en estos casos parte desde el primer momento de una presuposición: la consideración de los datos de tráfico y facturación como datos de carácter personal. De esta forma, en ningún momento se plantea nada al respecto. Claro está, ante esta ausencia de argumentación, resulta lógico concluir que tales datos son de carácter personal, por lo que la solución del problema formulado debe obtenerse a la luz de la legislación sobre protección de datos.

No obstante, la consideración de los datos de facturación y tráfico como parte integrante del objeto del secreto de las comunicaciones impide la admisión de la solución esgrimida por la Agencia. Precisamente, la mayor parte de la doctrina sobre el secreto de las comunicaciones se ha elaborado respecto de supuestos de escuchas y demás actos de las Fuerzas de Seguridad del Estado. A este respecto, la doctrina del Tribunal Constitucional adopta una posición restrictiva de sus posibilidades, como ya se ha visto anteriormente. Igualmente, el Tribunal Europeo de Derecho Humanos ha considerando injerencia la captación por tales fuerzas, no sólo de conversaciones, sino de la identidad de los sujetos que intervienen en ellas, mediante el conocimiento de los números marcados (caso Malone), lo que requiere el control judicial de tales actividades.

Desde el punto de vista de la protección de datos de carácter personal, no tranquiliza la alusión a la LOPJ, que exige la comunicación inmediata de los actos realizados y sus resultados a los Jueces y Fiscales. Tal exigencia no elimina el hecho de que, en realidad, son las Fuerzas de Seguridad las que llevan a cabo las operaciones de recogida y tratamiento, como se deduce expresamente del artículo 20, que la Agencia trae a colación. Es más, la expresión de este precepto *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,* hace suponer claramente que la notificación tiene como fin, además de la iniciación o continuación de las actuaciones procesales, la del control de los actos de recogida a través de una cesión y tratamiento de los datos realizados por los cuerpos policiales. Así, no se puede argumentar que el destino final de los datos y su tratamiento suponga, como parece pretender la Agencia con semejante argumentación, la existencia de una cesión a los Jueces y Fiscales, pues el paso de los datos por los ficheros policiales no es meramente anecdótico, sino que los mismos residen en aquéllos para satisfacer específicos fines policiales. En realidad, no creemos que estas cesiones encajen en el artículo 11.2 d), pues la Policía no actúa como mero puente. Se trata, más bien, de dos cesiones: una primera a la Policía y otra posterior a los citados órganos. Por lo tanto, desde la óptica de la protección de los datos de carácter personal, la primera cesión corresponde al supuesto del artículo 22 y la segunda al del artículo 11.2 d). No resulta insustancial la especificación de los preceptos aplicables, puede debemos tener en cuenta que el artículo 22 es mucho más exigente en las circunstancias que deben concurrir para habilitar la recogida y tratamiento de datos por la Fuerzas de Seguridad. Utilizar el artículo 11.2 para justificar estas cesiones aporta un peligro injustificado, ante la amplitud de posibilidades que la redacción simple de este precepto presenta.

En cualquier caso, entendemos que los supuestos planteados deben la satisfacer las exigencias derivadas de la protección del secreto de las comunicaciones, por las razones ya apuntadas, sobre todo si tenemos en cuenta la particular naturaleza de los supuestos y órganos que intervienen en los mismos, según ya hemos señalado.

3. Los datos de carácter personal en la facturación detallada.

La protección de la posición de los usuarios de servicios de telecomunicación exige el establecimiento de medios que faciliten la transparencia e información precisa del uso que de tales servicios realizan aquéllos. En este sentido, nadie discute que la obligación de facturación detallada impuesta a los operadores supone un avance en esa dirección. En este sentido, se estableció por la Directiva 98/10/CE, de 26 de Febrero de 1998, sobre aplicación de la oferta de red abierta (ONP) a la telefonía vocal y sobre el servicio universal de telecomunicaciones en un entorno competitivo, el derecho a la factura detallada. No obstante, el efecto positivo de la información puede conllevar, a la vez, consecuencias negativas. Concretamente, la transparencia de la información personal implica necesariamente también dicha transparencia respecto de los propios operadores, que pueden conocer mejor a los usuarios y gozan de mayores posibilidades mediante la tenencia de tal información. Lógicamente, algunas de esas posibilidades deben ser limitadas. De ahí, que la Directiva 2002/58/CE estableciera, en su artículo 7.1, el derecho a recibir facturas no desglosadas.

La protección de los datos personales[25] en la facturación detallada se contiene en el artículo 66 del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones. Según este precepto,

> *Los abonados tendrán derecho a recibir las facturas no detalladas cuando así lo soliciten a los operadores que, de conformidad con lo dispuesto en este Reglamento y en las Ordenes ministeriales que regulen las licencias individuales y las autorizaciones generales, tengan la obligación de prestar dicho servicio.*
>
> *Asimismo, por resolución del Secretario general de Comunicaciones se fijarán las distintas modalidades de facturación detallada que los abonados pueden solicitar a los operadores, tales como la supresión de un determinado número de cifras en la factura de los números a los que se ha llamado o la no*

[25] Aunque la denominación jurídicamente correcta es datos de carácter personal, sin embargo empleamos la expresión datos personales, pues es la que se utiliza en el encabezamiento del artículo 66. A pesar de la incorrección terminológica, se suelen utilizar ambas expresiones de modo indistinto, aunque algún autor, como Heredero Higueras, haya señalado las posibles diferencias entre aquéllas y la preferencia por la primera. HEREDERO HIGUERAS, MANUEL. *La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Comentario y textos.* Ed. Tecnos. MADRID, 1996. Pág. 71.

aparición en la factura de los números a los que se llama cuando el pago se haga con tarjeta de crédito, como mecanismos de garantía de la utilización anónima o estrictamente privada del servicio.

Una primera cuestión que surge, antes de analizar el precepto, es la relativa a la naturaleza de estos datos. Mejor dicho, es necesario preguntarse si la inclusión de estos datos de facturación en un documento de factura en un momento posterior al de su generación altera su naturaleza y, por tanto, el régimen jurídico aplicable. Como hemos señalado anteriormente, cuando nos planteamos si los datos de tráfico eran otro tipo de datos distinto a los datos de facturación, hemos de concluir que el transcurso del tiempo, después del acto de comunicación, así como la especificación del fin último de éstos mediante la formalización de la factura, en nada modifica sus caracteres. Por lo tanto, sobre la base de lo anteriormente manifestado, la información recogida en la factura detallada forma parte del ámbito de aplicación del derecho al secreto de las comunicaciones.

La redacción del artículo 66 no contradice tal opinión, pues en el mismo se regula un instrumento de información dirigido al abonado, no a posibles terceros, los cuales no tienen derecho por sí a acceder a la misma, sino que requerirían la autorización judicial para la cesión de dichos datos. Podría plantearse que el abonado que recibe la factura conociera información de tráfico y facturación relativa a comunicaciones que ha realizado un usuario distinto de aquél en su terminal. Tal posibilidad supondría la revelación de datos a persona distinta del afectado, es decir, del usuario concreto que realiza el acto de comunicación, lo que encaja con el concepto de cesión. No obstante, como ya hemos señalado, el Reglamento no permite la inclusión en la factura de datos relativos a los usuarios, lo que por otra parte, sólo sería técnicamente posible mediante la interceptación de la llamada, con lo que de nuevo se necesitaría la intervención judicial[26]. Por otra parte, la configuración como cesión de tal supuesto no conlleva consecuencias prácticas relevantes, en nuestra opinión, pues esta posibilidad, por la naturaleza de los datos, no se regiría por la normativa sobre protección de datos de carácter personal, sino por la atinente al secreto de las comunicaciones.

Ahora bien, aunque de la factura no se deduce claramente quien ha sido el sujeto que ha efectuado la llamada desde el terminal de que es el titular el abonado, sin embargo existen posibilidades de determinación indirecta de la información del primero, así como también se proporciona información sobre la parte de la

---

[26] Lejos de parecer carente de interés, esta cuestión pude revestir cierta importancia. Piénsese, por ejemplo, en todos aquellos casos en los que se efectúa una llamada desde un teléfono de un lugar público. En este sentido Cavanillas Múgica recuerda que el desglose de las facturas en ámbitos como el doméstico o el laboral, puede afectar a la protección de los datos de dichos usuarios. CAVANILLAS MUGICA, SANTIAGO. *Telecomunicaciones y protección de la intimidad personal en el seno del grupo doméstico.* XII Encuentros sobre Informática y derecho, 1998-1999. Universidad Pontificia de Comillas. Ed. Aranzadi. MADRID, 1999. Pág. 30.

comunicación. En este sentido, se produce una colisión entre los intereses del abonado de conocer el uso y la correcta facturación de sus comunicaciones y el derecho de los usuarios emisores o los abonados receptores a preservar su información frente a los primeros. Tal circunstancia se expresa con claridad en el artículo 7 de la Directiva 2002/58, según el cual

> 1. *Los abonados tendrán derecho a recibir facturas no desglosadas.*
>
> *2. Los Estados miembros aplicarán las disposiciones nacionales a fin de reconciliar los derechos de los abonados que reciban facturas desglosadas con el derecho a la intimidad de los usuarios que efectúen llamadas y de los abonados que las reciban por ejemplo, garantizando que dichos usuarios y abonados dispongan de suficientes modalidades alternativas de comunicación o de pago que potencian la intimidad.*

La preservación del secreto justifica la adopción de las medidas contempladas en el artículo 66, relativas a la supresión de parte del número al que se llama o la supresión de números cuando el pago se efectúa mediante tarjeta de crédito. Idénticas medidas se prevén en el Considerando 33 de la Directiva 2002/58, según el cual

> *La introducción de facturas desglosadas ha aumentado la posibilidad de que el abonado pueda comprobar que las tarifas aplicadas por el proveedor del servicio son correctas, pero, al mismo tiempo, puede poner en peligro la intimidad de los usuarios de los servicios de comunicaciones electrónicas disponibles al público. Por consiguiente, a fin de proteger la intimidad de los usuarios, los Estados miembros deben fomentar el desarrollo de opciones de servicios de comunicaciones electrónicas tales como posibilidades de pago alternativas que permitan el acceso anónimo o estrictamente privado a los servicios de comunicaciones electrónicas disponibles al público, por ejemplo tarjetas de llamada y posibilidad de pago con tarjetas de crédito. Con idéntico propósito, los Estados miembros también podrán pedir a los operadores que ofrezcan a sus abonados otro tipo de factura detallada e la que se omita cierto número de cifras del número llamado.*

La reproducción de este Considerando nos interesa bastante, porque, a pesar de las buenas intenciones manifestadas en el mismo y repetidas en la normativa interna, sin embargo su efectividad queda muy minimizada o, más bien, anulada. Como se puede observar, los términos empleados en el Considerando no imponen obligación alguna directa a los Estados miembros. Se dice que los Estados *deberán fomentar las opciones de servicios de telecomunicaciones* o que los mismos *podrán exigir*. Es decir, se deja la última decisión sobre el nivel de exigencia de tales posibilidades a los Estados. En este sentido, la normativa española no ha establecido con carácter imperativo dichas medidas sobre restricción parcial o total de números, según la forma de pago.

En efecto, como ya hemos visto anteriormente, el artículo 66 del Reglamento establece que los abonados *tendrán derecho* a solicitar facturas no detalladas o que *los abonados podrán solicitar* modalidades de facturación restringida. Por lo tanto, la protección de la Intimidad de los usuarios, en expresión utilizada por la Directiva, se abandona, en última instancia, a la decisión de los abonados de cada terminal, que podrán satisfacer tal protección o no. Mucho nos tememos que, en la mayoría de los casos, tales abonados desean tener la mayor cantidad de información posible, por lo que el nivel efectivo de protección será nulo. Precisamente por estas razones, resulta más conveniente la configuración de los datos de tráfico y facturación como elementos integrantes del secreto de las comunicaciones. Desde este punto de vista, no existe obstáculo alguno al conocimiento por una de las partes de la información sobre los usuarios que efectúan la llamada o los abonados que la reciben, pues como vimos anteriormente, no existe deber de secreto entre las partes que conforman tal comunicación, según manifestó el Tribunal Constitucional. Sin embargo, desde la óptica de la protección de los datos de carácter personal, las soluciones adoptadas presentan problemas conceptuales, ante la inaplicación de las medidas que requiere la protección de dicho bien jurídico.

Podría plantearse que, en el supuesto de que un usuario utilice el teléfono de otro abonado para una comunicación, el detalle en la factura de dicha comunicación implicaría conocimiento por un tercero de la misma. Ahora bien, en ningún caso se podría hablar de interceptación de la comunicación, que es el acto que requiere la autorización judicial. Hemos de tener en cuenta que la interceptación requiere una actuación positiva en tal sentido por parte del tercero, con independencia del momento en el que se produce tal interceptación o conocimiento[27]. En el supuesto de conocimiento por medio de la factura, dicho abonado no hace nada sobre el acto de comunicación, sino que, de forma pasiva, recibe esta información. Partiendo de dicho presupuesto, es el posible usuario quien debe tener en cuenta tal circunstancia, debe ser diligente en la protección de la información que le atañe.

4. La utilización de los datos de facturación para fines de promoción comercial.

[27] Como señala la Fiscalía General del Estado, en contra de lo que propugnaba el Abogado del estado en las alegaciones recogidas en la sentencia 114/1984, el secreto de las comunicaciones extiende su ámbito más allá del momento preciso en el que se produce la comunicación. Posición que refuerza la sentencia citada, en la que se afirma que tal secreto se vulnera tanto por la interceptación de la comunicación, la cual debe producirse en tiempo real, como por el conocimiento antijurídico de su contenido, por ejemplo, según cita expresamente la sentencia, mediante la apertura de correspondencia de correspondencia guardada por el destinatario. Este último supuesto supone que la comunicación ya ha concluido, pues el soporte en que se materializa la comunicación ya se ha recibido. En el mismo sentido, señala el Tribunal Constitucional que el secreto de las comunicaciones protege el proceso de comunicación y el mensaje, entendido éste como contenido de aquélla, el cual puede perdurar en el tiempo respecto de alguno de sus elementos, como la identidad de las partes.

El artículo 65.3 del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones establece que

> *Asimismo, los operadores podrán tratar los datos a que se refiere el apartado anterior para la promoción comercial de sus propios servicios de telecomunicaciones, siempre y cuando el abonado haya dado su consentimiento previo. A estos efectos, los operadores deberán dirigirse a los abonados, al menos, con un mes de antelación al inicio de la promoción, requiriendo su consentimiento que, de producirse, será valido hasta que los abonados lo dejen sin efecto de modo expreso. Si en el plazo de un mes desde que el abonado reciba la solicitud, éste no se hubiere pronunciado al respecto, se entenderá que consiente, sin perjuicio de lo dispuesto en la disposición transitoria séptima*[28].

La regulación del artículo 65.3 del Reglamento pudiere resultar contradictoria con la configuración de los datos de facturación como parte del ámbito de protección del secreto de las comunicaciones. En este artículo se establece la necesidad de que el operador cuente con el consentimiento de los abonados para el posterior uso comercial de aquellos datos. Parece claro que se exige la concurrencia de un requisito que es propio y fundamental de la protección de datos de carácter personal, cual el consentimiento del afectado como medio de control sobre sus datos. En este sentido, en la práctica la aplicación de este precepto se ha realizado aludiendo a la legislación de protección de datos, de manera que los operadores telefónicos han solicitado el consentimiento de los afectados por carta, señalando que se hacía en cumplimiento de tal normativa. Por otra parte, el artículo 18.3 de la Constitución permite la limitación del secreto de las comunicaciones cuando media autorización judicial, sin que se haga alusión alguna a la concurrencia del consentimiento de alguno de los participantes en el proceso de comunicación. En definitiva, parece que todo induce a pensar que el uso de los datos de facturación es materia propia de la protección de los datos personales. Pero claro está, esto negaría la consideración de los datos de facturación como parte del proceso de comunicación, inmersos en la misma como elemento del mismo bien jurídico.

Respecto de lo anterior, vuelve a surgir el interrogante sobre la extensión temporal de las comunicaciones, más allá de su duración. También es necesario preguntarse sobre el papel de los operadores telefónicos, los cuales, no siendo parte en las conversaciones telefónicas, conocen datos que, según se ha afirmado, son parte de aquéllas. Por otra parte, resulta conveniente analizar si la modificación en el destino de los datos puede suponer igualmente la alteración de su régimen jurídico.

---

[28] Tal disposición rige para aquellos supuestos en los que el tratamiento para fines comerciales de los datos de tráfico y facturación se haya iniciado con anterioridad a la entrada en vigor de este Reglamento. En tal caso, según establece la Disposición Transitoria séptima, se deberá comunicar tal tratamiento a los abonados en el plazo de dos meses desde la entrada en vigor. Si éstos no se oponen en el plazo del mes siguiente, se entiende que consienten tal tratamiento.

La cuestión relativa a la extensión temporal del secreto de las comunicaciones, no plantea grandes dudas. Como ya se dijo anteriormente, la terminación del proceso de comunicación no supone la inaplicación del secreto de las comunicaciones. Según ha señalado el Tribunal Constitucional, el bien jurídico que se pretende proteger en este caso es la libertad de las comunicaciones. Obviamente, la relajación de la protección en momentos posteriores a la comunicación no va en favor de dicha libertad. Por lo tanto, no existe problema alguno en extender las exigencias del secreto más allá del momento preciso de las comunicaciones.

No obstante lo anterior, la exigencia del consentimiento parece estar en consonancia, más con la protección de datos de carácter personal que con el secreto de las comunicaciones. Respecto de este punto, hemos de señalar que la autorización judicial supone un refuerzo en la protección de las comunicaciones, pero en nada excluye la posibilidad de que las partes puedan voluntariamente permitir el acceso a la comunicación y a su contenido por parte de terceros. En realidad, se trataría de la aplicación a este supuesto de la doctrina emanada del Tribunal Constitucional, según la cual el secreto de las comunicaciones no vincula a los participantes en las mismas. De esta forma, los abonados podrían ofrecer la posibilidad de usar esta información, mediante su consentimiento, sin necesidad de que concurra voluntad alguna de los usuarios en tal sentido. Así, aunque las expresiones utilizadas por el precepto se acercan más a los modos empleados en la regulación sobre protección de datos de carácter personal, sin embargo la misma corrección formal, y por supuesto mayor corrección material, se observa en la concepción de tal información como contenido de las comunicaciones. Obviamente, la concurrencia del consentimiento del abonado elimina la necesidad de la intervención judicial, pues sus manifestaciones no requieren la aprobación del Juez, al no incluirse tal supuesto, como ya se ha dicho, en el ámbito protegido por el secreto de las comunicaciones.

Claro está, todo lo anterior sirve en el caso de que se sostuviera que el operador telefónico es un tercero respecto del proceso de comunicación. Pero lo cierto es que el operador, aunque no interviene en aquélla, sin embargo conoce de modo inmediato, incluso antes que los comunicantes, alguno de los datos de facturación: tiempo de la llamada, coste, etc. Debemos tener en cuenta que los operadores no son terceros en el sentido expresado por la doctrina del Tribunal Constitucional. En realidad, no se trata tanto de posibles terceros que pudieren acceder a la comunicación como del vehículo que facilita ésta. El conocimiento del destinatario de una llamada telefónica por parte de dichos operadores es necesario si deseamos comunicar con alguien, dado que, por la naturaleza de las cosas, se debe conocer previamente quien pretende comunicar y con quién se quiere comunicar. Además, la prestación del servicio implica la asunción por parte de los abonados de que los operadores puedan conocer las características del acto de comunicación, pues en caso contrario no se posibilitaría tal servicio. En definitiva, el acceso a tal información por los operadores es presupuesto o medio necesario para la efectividad de la comunicación, de manera que no se puede excluir tal facultad de los operadores:

no es una injerencia externa en la comunicación en curso, sino un presupuesto necesario para que ésta tenga lugar.

Ya hemos visto que la protección que brinda el secreto de las comunicaciones se extiende más allá del estricto plazo de aquéllas. Ahora bien, lo cierto es que, en el caso que nos ocupa, se observa alguna diferencia entre los datos de facturación en los momentos previos, desde su generación en tiempo real hasta su utilización para el cobro del servicio, y su posterior uso fuera de los fines iniciales que justificaron su recogida y almacenamiento. Hasta ahora, en páginas y epígrafes anteriores hacíamos referencia al tratamiento de los datos de facturación con la finalidad de satisfacer precisamente dicho fin, la determinación exacta del coste del servicio y la exigencia de su pago a través de la factura. Sin embargo, observamos que, en el supuesto presente, se amplían las finalidades del tratamiento de estos datos, pues se trasciende a la finalidad primitiva para satisfacer objetivos de naturaleza comercial.

En el supuesto del tratamiento de los datos de facturación con fines de publicidad se produce una alteración en los fines perseguidos con aquél que provoca que nos planteemos si, a la vez, se produce una modificación del bien jurídico que se debe proteger frente a esos usos. En el caso del tratamiento con fines de facturación, se pretendía proteger la libertad de las comunicaciones. En este sentido, la facturación era una consecuencia necesaria de la utilización del servicio de telecomunicación, pues no hay factura de llamadas si no hay realización de dichas llamadas, lo que permite extender la protección que se brinda a las mismas a sus consecuencias. Sin embargo, en el caso de la explotación comercial de tales datos ya no se pretende conocer y analizar los actos de comunicación y su contenido, sino deducir las posibilidades comerciales futuras que las mismas manifiestan de forma indirecta. Es decir, se produce una modificación de los objetivos, que implica también una nueva perspectiva jurídica del problema. Así, podría pensarse que tal explotación de datos ya no vulnera la libertad de las comunicaciones, sino que, más bien, supone un potencial peligro para la protección de los datos de carácter personal. Sin embargo, tenemos serias dudas al respecto, pues el simple cambio de fines por parte de quien trata los datos no debe suponer la sustitución del régimen jurídico, dado el posible debilitamiento de la protección que la misma pudiere conllevar.

La aplicación al tratamiento comercial de los datos de facturación de la legislación de protección de datos se justifica con mayor corrección desde otro punto de vista. Como hemos visto en líneas anteriores, los operadores telefónicos facilitan o permiten los actos de comunicación, son un presupuesto necesario de los mismos. De esta manera, su participación, que supone el conocimiento de determinados datos, no se configura como una interceptación en sí. Tal posibilidad se predica de quien pretende conocer tanto el hecho como el contenido de la comunicación, sin participar en ella, mientras que el operador tan sólo ofrece el servicio. En realidad, no intercepta comunicación alguna, sino que conoce previamente ciertos datos, como consecuencia de la naturaleza de sus actividades. Tal conocimiento de los datos de facturación se justifica porque, como parte en el contrato de prestación del servicio telefónico, tiene

derecho a conocer las circunstancias de las comunicaciones efectuadas. Resulta lógico que se deban proporcionar medios seguros para el pago de los servicios a quien proporciona tal servicio. Por esta razón, el conocimiento de los datos de facturación se fundamenta en el consentimiento genérico del abonado al contrato y a las obligaciones derivadas del mismo.

En relación con lo anterior, señala Fernández Esteban que los proveedores y operadores pudieran configurarse como "terceros cualificados". Para ello, se apoya en la legislación de correos y de telecomunicaciones, las cuales establecen, no obstante, normas restrictivas al respecto: el Decreto 1653/1964, de 14 de Mayo, permite la apertura del correo para averiguar el destino (la autora reconoce la posible inconstitucionalidad), el artículo 51 de la LGT permite conocer los datos de tráfico y facturación para garantizar la utilización del dominio público radioeléctrico[29].

Es precisamente esta previa relación contractual el elemento diferenciador del papel de los operadores respecto de terceros ajenos a la comunicación. Como se ha dicho, son éstos últimos los que, con su intervención, pueden dar lugar a actos de interceptación, no así los primeros, cuya actuación se legitima por el consentimiento contractual inicial. De todo lo anterior se puede extraer una importante conclusión: la delimitación del régimen jurídico aplicable al tratamiento de los datos de facturación, en cada caso, así como de los derechos contemplados en los artículos 18.3 y 18.4 de la CE, requiere la utilización de un criterio subjetivo. La intervención de las comunicaciones por terceros ajenos requiere la autorización judicial, por ser constitutiva de interceptación. Por el contrario, la actuación de los operadores no es equiparable al supuesto anterior, pues tal intervención ha sido prevista por los abonados, lo cual excluye la aplicación del artículo 18.3 de la CE.

Ahora bien, la legitimación contractual del tratamiento de los datos de facturación no amplía de modo indefinido las posibilidades de los operadores. La delimitación del objeto del contrato y las obligaciones asumidas por las partes en éste, permiten el tratamiento con fines de facturación, al ser estas operaciones presupuesto necesario de la ejecución del contrato. Tal uso está en consonancia con lo dispuesto por el artículo 6.2 de la LOPD, según el cual

> *2. No será preciso el consentimiento cuando los datos de carácter personal …cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;…*

Sin embargo, el caso que nos ocupa se refiere a un uso de los datos que no es imprescindible para que el operador obtenga la satisfacción de su derecho, es

---

[29] FERNANDEZ ESTEBAN, MARIA LUISA. *Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las comunicaciones entre particulares, en especial en el ámbito de la empresa.* Aranzadi Civil, núm. 3. Mayo de 2000. Pág. 1893.

decir, para ejecutar la obligación de pago. Así, salvo previsión expresa en el contrato, la utilización comercial de los datos de facturación requiere consentimiento del abonado, como exige el artículo 65.3 del Reglamento de desarrollo de la Ley General de Telecomunicaciones, al no ser tal tratamiento requisito necesario para la ejecución del contrato, a la vez que tal uso trasciende a la finalidad inicialmente prevista. Parecidos argumentos se han sostenido en la sentencia de la Audiencia Nacional (Sala de lo contencioso-administrativo, sección 1ª), de 6 de Julio de 2001. Por ello, sostiene la Agencia Española de Protección de Datos que es necesario que en el contrato debe hacerse constar de forma expresa la posibilidad de que el usuario se pueda oponer al tratamiento de sus datos con los mencionados fines[30].

Todas las anteriores razones nos permiten afirmar que la utilización de los datos de facturación, con el consentimiento de los abonados, excluye la aplicación del régimen jurídico relativo al secreto de las comunicaciones y habilita el control del uso que se vaya a hacer de los datos, en este caso con fines de prospección comercial, a través de la regulación de protección de datos de carácter personal. No debe considerarse que la interpretación realizada está condicionada a priori por los resultados que, según la opción elegida, se puedan obtener. Por el contrario, ya hemos señalado que los datos de facturación incluyen información de carácter personal, que justificaría el tratamiento jurídico de los mismos desde la óptica de la protección de datos de carácter personal. El matiz que permite desdoblar la solución en cada caso es la configuración de tales datos como elemento del proceso de comunicación y además, la finalidad de los posibles usos, lo que permite conectar o no, en su caso, con el derecho al secreto de las comunicaciones del artículo 18.3 de la Constitución.

5. Los datos de carácter personal existentes en el mensaje o contenido en sentido estricto de la comunicación.

A la luz de la sentencia del Tribunal Constitucional de 29 de Noviembre de 1984, anteriormente reseñada, se podría llegar a la conclusión de que los datos de tráfico y facturación encajan en el ámbito de protección que proporciona el derecho fundamental al secreto de las comunicaciones, de forma más correcta que en el propio de la protección de datos de carácter personal. Sin embargo, pudiera ocurrir entonces que, según la doctrina esgrimida por el Tribunal Constitucional en la mencionada sentencia, la consecuencia práctica fuera precisamente un menor grado de protección para los datos de carácter personal que no se generen durante la comunicación para fines de facturación. Por las propias circunstancias del caso planteado, la Fiscalía General del Estado no se planteó tal posibilidad, pues se estaba debatiendo sobre la cesión de datos a un tercero, sin entrar a analizar las facultades de los intervinientes en la comunicación respecto de otro tipo de datos no contemplados en este caso. Sin embargo, nosotros debemos analizar tal supuesto, pues si bien la posición de la Fiscalía pudiera otorgar una mayor protección de la comunicación frente a terceros,

---

[30] *Informe de la Agencia Española de Protección de Datos sobre las cláusulas para el consentimiento al tratamiento de los datos en los contratos de prestación de servicios telefónicos.* www.agpd.es.

sin embargo conllevaría la consecuencia contraria respecto de las partes en la comunicación.

Como se ha visto anteriormente, la sentencia del Tribunal Constitucional mencionada consagra la inaplicación del deber de secreto en las comunicaciones respecto de las partes que en la misma intervienen. Consecuencia de lo anterior, se afirma en aquélla que la grabación y la posterior divulgación no implican la vulneración de dicho derecho fundamental. Pues bien, la consideración de los datos de carácter personal vertidos en la comunicación como uno de sus elementos sin mayor detenimiento, dado que los mismos forman parte del mensaje, conllevaría la consecuencia de que los mismos podrían ser recogidos y divulgados por el receptor sin limitación alguna. Esta conclusión no puede ser admitida, pues implicaría el absurdo de reducir las garantías que la legislación sobre protección de datos establece respecto de los mismos.

Tal posibilidad ya fue prevista por el Tribunal Constitucional en 1984. Aunque el mismo no tuvo ni podía tener en cuenta la regulación de los datos de carácter personal, pues por aquel entonces ni siquiera habría entrado en vigor el Convenio nº 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[31], sin embargo sí reconoció que la solución jurídica era diferente cuando el contenido de las conversaciones pudiere afectar a la Intimidad de alguna de las partes, conforme se deduce de las partes de la sentencia extractada en páginas anteriores.

Como se puede deducir de la doctrina del Tribunal Constitucional, la posibilidad de la libre difusión del contenido de una comunicación por las personas que participan en ella, no extiende a todos aquellos contenidos que afectan a la esfera íntima de la persona. Según ya se ha dicho anteriormente, la novedad de la protección de los datos de carácter personal imposibilitaba la alusión en tal sentido por parte del Tribunal Constitucional. Ahora bien, no cabe duda que el bien jurídico protegido en el artículo 18.4, si bien no se refiere exclusivamente a la información más íntima de un sujeto, sin embargo tiene en común con los datos de tal naturaleza su referencia en cualquier caso a información relativa a una persona, siquiera con un diferente grado de sensibilidad, lo que, en cualquier caso, manifiesta una cercanía de los bienes jurídicos que se protegen en cada caso.

Tal carácter personal parece excluirse por el alto Tribunal del ámbito del secreto de las comunicaciones, pues es de suponer que, de conocer y tener en cuenta el Tribunal Constitucional la legislación de protección de datos en la época de la sentencia, hubiese concluido en la diferencia de bienes jurídicos protegidos por ésta última y el derecho al secreto de las comunicaciones y, así, en la separación de los regímenes aplicables en cada caso. Según esta conclusión, los datos de carácter personal vertidos en una comunicación quedan extramuros de la protección del

[31] Este Convenio está fue ratificado por España por Instrumento de 27 de Enero de 1984 y publicado en el BOE de fecha 15 de Noviembre de 1985.

artículo 18.3 de la CE[32]. En la práctica, la solución no puede ser otra. En relación con la protección de datos de carácter personal, hoy día son comunes las encuestas telefónicas y los servicios prestados por este mismo medio, en los que los receptores de la llamada suelen proporcionar aquéllos. La especialidad del medio de recogida, la comunicación, no puede conllevar la total disponibilidad de los mismos por parte de sus solicitantes. Si así fuera, la consecuencia inmediata no sería otra que la postura negativa de los usuarios, lo que implicaría la imposibilidad de explotación de los medios de comunicación para tales fines y los beneficios que supone. Si ya de por sí el modo de comunicación telefónico provoca una desconfianza en los usuarios (por ejemplo, las dudas respecto de la identidad real de quien solicita los datos), no deben rebajarse sus garantías ni el grado de protección.

Pues bien, si los datos de carácter personal que se manifiestan en la comunicación se encuadran en el ámbito del artículo 18.4 y no del artículo 18.3, podría entenderse lo mismo respecto de los datos de tráfico y facturación, pues la información que se deduce de éstos puede ser idéntica a la que contienen aquéllos. Sin embargo, no parece que la asimilación de ambas soluciones resulte válida. Se debe tener en cuenta que, en los casos propuestos de encuestas telefónicas y similares, la finalidad es la recogida de los datos solicitados con el fin de someterlos a unas operaciones de tratamiento para la consecución de los objetivos pretendidos (comerciales, estadísticos o de otra naturaleza), y en tal sentido el solicitante de los datos expresa sus intenciones a quien se solicita que proporcione dichos datos. En fin, la diversidad y diferencia de dichos objetivos determina que la solución normativa sea también diversa.

6. Los datos de carácter personal de datos contenidos en las guías telefónicas.

El artículo 3 j) de la LOPD, en la definición sobre las fuentes accesibles al público, acoge una lista cerrada de las mismas, entre las que se encuentran los repertorios telefónicos. Como señala el precepto, estas guías se rigen por la legislación sobre la materia, en este caso, la legislación sobre telecomunicaciones. En realidad, el análisis de los repertorios telefónicos forma parte del estudio de las fuentes accesibles al público. Sin embargo, en este caso se observan una serie de especificidades que justifican un tratamiento separado de aquéllos. Así, hemos de profundizar en algunas cuestiones que han surgido exclusivamente a la luz de estos repertorios.

a. La regulación sectorial de las guías telefónicas.

La LOPD no contiene una regulación expresa sobre esta materia, solamente acoge un precepto de remisión a la normativa sectorial. Según el artículo 28.4,

---

[32] Efectivamente, la contestación a este planteamiento requiere analizar cuál es el bien jurídico realmente protegido por el artículo 18.4 de la CE y la legislación de desarrollo. No obstante, por razones de corrección sistemática y extensión, dejamos tal estudio para otra ocasión.

> *Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.*

Por su parte, la normativa sobre telecomunicaciones contiene una regulación dispersa y profusa relativa a las guías telefónicas. En primer lugar, la Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones contiene dos artículos a este respecto. Por una parte, el artículo 37.1 b) de la Ley General de Telecomunicaciones establece que el servicio universal de telecomunicaciones impone, entre otras obligaciones,

> *Que los abonados al servicio telefónico dispongan, gratuitamente, de un guía telefónica, actualizada e impresa y unificada para cada ámbito territorial. Todos los abonados tendrán derecho a figurar en las guías y a un servicio de información nacional sobre su contenido, sin perjuicio, en todo caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad.*

Por otra parte, el artículo 54, relativo a los derechos de los usuarios, establece en su apartado 3º:

> *Sin perjuicio de lo establecido en el artículo 37. b), la elaboración y comercialización de las guías de abonados a los servicios de telecomunicaciones se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías.*

En definitiva, la Ley reconoce, de modo general, la protección de los datos de carácter personal de los abonados contenidos en las guías telefónicas[33]. Sin embargo, el conocimiento del régimen de esta protección exige acudir al desarrollo reglamentario. El Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones hace referencia a las guías telefónicas en los artículos 14 y 67. El

---

[33] Podría pensarse que tal reconocimiento no implica ninguna novedad respecto de las regulaciones anteriores. Sin embargo, en épocas relativamente recientes los abonados no gozaban de todos los derechos ahora reconocidos, ni éstos tenían, en su caso, la misma extensión. Por ejemplo, la resolución de 9 de Julio de 1982, de la Delegación del Gobierno en CTNE (antigua Telefónica pública), establecía que la aparición en las guías era obligatoria, de manera que sólo se permitía la exclusión cuando el abonado ya figuraba en la guía por otro teléfono instalado en el mismo domicilio o cuando lo aconsejaren circunstancias especiales concurrentes en el caso. Es decir, se admitía la posibilidad de la exclusión de modo muy restrictivo, a diferencia del régimen actual, en el que los abonados pueden ejercer tal derecho por su sola voluntad, sin necesidad de acreditar circunstancias análogas a las citadas. En el mismo sentido, CARRASCO PERERA, ANGEL, MENDOZA LOSANA, ANA I. e IGARTUA ARREGUI, FERNANDO. *Comentarios a la Ley general de telecomunicaciones.* ARPON DE MENDIVIL ALDAMA, ALMUDENA y CARRASCO PERERA, ANGEL (Directores). Ed. Aranzadi. PAMPLONA, 1999. Pág. 630.

primero de estos preceptos, referido de modo general a las guías telefónicas, dispone en su apartado 1º:

> *Los abonados al servicio telefónico fijo disponible al público tendrán derecho a disponer de una guía telefónica de carácter gratuito, unificada para cada ámbito territorial, que será, como mínimo, provincial. Asimismo, tendrán derecho a figurar en la guía y, en su caso, a solicitar la corrección o supresión de los datos relativos a ellos. Estas guías deberán estar a disposición de todos los usuarios y ser actualizadas periódicamente. Mediante Orden del Ministerio de Fomento se fijarán los criterios para su elaboración, actualización y los datos que deberán figurar en ellas.*

Con el encabezamiento *Guías de servicios de telecomunicaciones disponibles al público,* establece el artículo 67 las normas atinentes a la protección de datos de carácter personal que figuren o puedan figurar en las mismas. Dice este artículo:

> *1. Los datos personales que figuren en las guías de abonados de los servicios a los que se refiere el artículo 62 que sean accesibles al público o que puedan obtenerse a través de servicios de información, ya sean impresas o electrónicas, deberán limitarse a los que se dan estrictamente necesarios para identificar a un abonado concreto. Por orden del Ministerio de Fomento se determinarán las condiciones para hacer constar dichos datos.*
>
> *No obstante lo dispuesto en el párrafo anterior, los operadores encargados de la elaboración de las guías podrán publicar otros datos personales de los abonados siempre que éstos hayan dado su consentimiento inequívoco.*
>
> *A estos efectos, se entenderá que existe consentimiento inequívoco del abonado, cuando se dirija al operador por escrito solicitándole que amplíe sus datos personales que figuran en la guía. También se producirá cuando el operador solicite al abonado su consentimiento y éste le responda en el plazo de un mes dando su aceptación. Si en dicho plazo el abonado no hubiese dado su consentimiento expreso, se entenderá que no acepta que se publiquen en la guía correspondiente otros datos que no sean los que se establecen en el párrafo primero de este apartado.*
>
> *2. Los abonados podrán exigir a los operadores que se les excluya de las guías, que se indique que sus datos personales no puedan utilizarse para fines de venta directa o que se omita parcialmente su dirección. Los operadores requeridos deberán cumplir lo dispuesto en este apartado, sin coste alguno para los abonados.*
>
> *Los abonados que soliciten su exclusión de las guías, tendrán derecho a recibir la información adicional a la que se refiere el párrafo segundo del apartado 3 del artículo 69*[34].

[34] Algún autor ha criticado la utilización de una norma de rango reglamentario para regular aspectos de la protección de datos personales que parecen requerir un precepto superior. En

b. Las cesiones o comunicaciones de estos datos.

Conforme se deduce del artículo 11.2 b) de la LOPD, la cesión de datos provenientes de las fuentes accesibles al público no requiere el consentimiento del abonado. Aunque este trabajo no se centra únicamente en el estudio de las cesiones de datos de carácter personal, sin embargo resulta de importancia analizar las posibilidades de inclusión de datos de carácter personal en las mismas, como límite objetivo a las cesiones que se vayan a realizar. Por otra parte, la simple aparición de tales datos en estas fuentes accesibles al público, permite encajar estos actos dentro de la definición que la LOPD contiene de la cesión, aún cuando los requisitos generales de éstas se hayan eliminado para la satisfacción del cumplimiento del fin de acceso generalizado. Por lo tanto, el exceso de información contenido en las guías, más allá de lo permitido por sus normas reguladoras, constituye un supuesto de cesión o comunicación, término más apropiado a este supuesto en cuanto alude a la mera

---

efecto, el Reglamento de desarrollo de la Ley General de Telecomunicaciones, aunque sea como consecuencia de la remisión de ésta última, establece el régimen de cuestiones que pudieren afectar al contenido esencial de un derecho fundamental. En este sentido, *vid.* ASPAS ASPAS, JOSE MANUEL. *Las guías de servicios de telecomunicaciones y la protección de datos.* La Ley, núm. 1. 2000. Pág. 1546.

No obstante la corrección formal de las anteriores afirmaciones, sin embargo no entendemos que en el presente caso se esté vulnerando el principio de jerarquía normativa. Hemos de recordar que la Ley General de Telecomunicaciones, al remitirse al Reglamento, exige la adecuación de la regulación a la LOPD, como norma general sobre la materia. En realidad, parece que el Reglamento establece una serie de preceptos que aportan soluciones concretas sobre cuestiones ya previstas de modo general en la legislación general, aplicable por remisión de la Ley sectorial. Las excepciones al consentimiento para tratar datos de tráfico y facturación, la necesidad del mismo cuando el tratamiento persiga satisfacer fines comerciales, el régimen de las guías y demás, especifican las soluciones generales de la LOPD, que, por ejemplo, establece el régimen del consentimiento y sus excepciones (con el cual encajan los preceptos del Reglamento) o la consideración de las guías como fuentes accesibles al público (lo cual amplía las posibilidades respecto de las mismas). En realidad, el Reglamento de desarrollo de la Ley General de Telecomunicaciones, desarrolla igualmente la LOPD, a la vez que su regulación es una transcripción casi literal de la Directiva 97/66. El Reglamento adopta, conforme establece el artículo 34 (antiguo artículo 50) de la Ley General de Telecomunicaciones, una serie de medidas técnicas que se adaptan perfectamente a la normativa general y a la LOPD. Aunque afecta a partes sustanciales de derechos fundamentales, lo hace en desarrollo de aquéllas y con pleno respeto a las mismas. Cuestión diferente es la idoneidad o no de las soluciones normativas adoptadas, como vamos a ver. Sobre estas cuestiones, MARTIN-RETORTILLO BAQUER, LORENZO. *Comentarios a la Ley General de Telecomunicaciones (artículo 50). Coord. Eduardo García de Enterría y Tomás de la Quadra-Salcedo.* Ed. Civitas. Madrid, 1999. Pags. 436-441.

Quizás, los problemas derivados de la jerarquía normativa se hubiesen evitado si la protección de datos se hubiese contenido de modo completo en la LOPD, sin separar las regulaciones por razón del ámbito. Ahora bien, es cierto que las telecomunicaciones presentan suficientes especialidades para justificar tal tratamiento separado, como se deduce de la actuación de los legisladores comunitario y español, según se ha visto.

posibilidad de conocimiento de dicha información, que no sería acogido por la normativa sobre dichas fuentes, lo que implicaría la aplicación de la normativa general sobre cesiones. No se puede deducir otra conclusión de la necesidad de que, según el artículo 67, sea necesario que el abonado preste su consentimiento para la inclusión en las guías de otros datos de carácter personal que no sean estrictamente necesarios para la identificación personal: se trata de un consentimiento para la revelación de tales datos, para su cesión por tanto, no para su tratamiento[35]. En relación con esta cuestión, resulta necesario averiguar cuáles son esos datos necesarios para la identificación de los abonados. Como dispone el artículo 67.1, tal determinación se efectuará por Orden ministerial.

En relación con lo anterior, cabe preguntarse si el dato relativo a la dirección del abonado es estrictamente necesario para su identificación. La finalidad directa de dicha información es la determinación de la ubicación del domicilio de aquéllos. Obviamente, el conocimiento del domicilio de los abonados ofrece una información que determina de modo más preciso quienes son aquéllos, en cuanto los sitúa en un lugar concreto. Por otra parte, resulta relativamente usual que los nombres y apellidos de los abonados sean idénticos a los de otros que figuran en las guías. Desde este punto de vista, la precisa identificación puede requerir el dato de la dirección, para poder distinguir cada uno de aquéllos. No obstante, no parece que la solución sea tan sencilla.

De los preceptos anteriormente recogidos sobre guías se deduce que la finalidad de las mismas es facilitar a los abonados el uso de los medios telefónicos, al proporcionar la información contenida en las mismas. Ahora bien, tal información debe estar condicionada a la satisfacción de dichos fines, es decir, se justifica la aparición de la información relativa al equipo telefónico (el número) y el abonado a quien pertenece y con quien se desea comunicar. En nada aumenta la identificación del abonado, salvo los casos de identidad de nombre y apellidos, el conocimiento de la dirección, dado que dicha identificación se permite a los exclusivos efectos de conseguir comunicar con aquél. Por otra parte, la distinción de las personas que coinciden en sus datos identificativos podría realizarse mediante el uso de datos añadidos abstractos, que no faciliten mayor información innecesaria para la comunicación. A este respecto, el artículo 53.1 de la Ley del Registro Civil establece:

> *Las personas son designadas por su nombre y apellidos, paterno y materno, que la Ley ampara frente a todos*[36].

---

[35] Quizás, el principal interés de este precepto radica en las exigencias establecidas respecto del consentimiento de los abonados.

[36] Este precepto de la Ley del Registro Civil no se ha visto afectado, curiosamente, por la Ley 40/1999, de 5 de Noviembre, que modifica determinados preceptos de aquélla relativos al nombre y apellidos y su orden.

Según se deduce del Preámbulo de esta Ley, la pretensión que se persigue es que el nombre sea un signo distintivo de los sujetos a quienes pertenece. En este sentido, si la Ley que contiene la normativa general sobre la identificación o distinción de los sujetos solamente utiliza el nombre y los apellidos con tal fin, no se entiende qué razón puede existir para que una normativa sectorial, determinada por la finalidad concreta del instrumento que regula, como son las guías, amplíe los datos que son necesarios para identificar a los abonados. Como hemos señalado, se trata de identificar para facilitar las comunicaciones, sin que esté justificada la inclusión de datos que excedan de dicho fin.

Podría sostenerse, no obstante, que tal información permite satisfacer fines legítimos. Por ejemplo, puede resultar conveniente a los efectos de la determinación exacta del domicilio de un sujeto, para evitar que las equivocaciones sobre éste puedan impedir el efecto perseguido por las notificaciones de un procedimiento administrativo. Sin embargo, la consecución de tal objetivo se justifica por la existencia de un interés legítimo, el cual no parece que deba satisfacerse por un medio de divulgación tan general como las guías, dado que tal interés no concurre en todos aquéllos que puedan consultarlas. Es decir, parece que las fuentes accesibles al público no deben servir para satisfacer intereses concretos, sino generales. En estos casos, está justificada la autorización, en el curso del proceso, para el uso de otros medios más específicos.

La finalidad de las guías telefónicas no va referida a la determinación de las líneas telefónicas en sí mismas, sino en cuanto éstas están referidas a sus titulares. Sólo así resulta posible conseguir el efecto de facilitar las comunicaciones. Por lo tanto, no sería admisible la afirmación de que la dirección persigue la ubicación, ni de las líneas ni del abonado, pues no es necesario situar aquélla y éste con tal propósito. La finalidad de información general para facilitar la comunicación se satisface exclusivamente con la aparición en las guías de los datos que precisamente permiten conseguir aquélla: el número de teléfono conectado a la persona del abonado con quien se desea comunicar. En el bien entendido de que tal fin no se puede satisfacer de manera plena, dado que la información sobre los usuarios que habitan la casa en la que está instalada la línea telefónica, no se proporciona por estas guías. Luego, si no se facilita información personal necesaria para realizar las llamadas, lo que parece ser el fin de estos medios de información, menos razón encontramos para justificar una información que para nada incide en esa misma dirección.

En el mismo sentido, la legislación sólo exigía, en un primer momento, la confección de las guías telefónicas para albergar números de telefonía fija. Es cierto que la permanencia de los anteriores no se corresponde con la variabilidad existente en el ámbito de la telefonía móvil. Las guerras de precios de los distintos operadores, pues se trata de un sector con un mayor grado de competencia en estos momentos, así como las insistentes campañas de publicidad y marketing, han provocado la explosión de su uso y el cambio, más o menos regular, de aparatos y líneas por los usuarios. Estos factores impiden la posibilidad de la determinación más o menos estable de las

líneas y sus abonados. No obstante, a este respecto debemos tener en cuenta las previsiones recogidas en la Orden del Ministerio de Ciencia y Tecnología 711/2002, de 26 de Marzo, que veremos en líneas posteriores.

La cuestión relativa a la información pertinente a los efectos de la comunicación se agrava cuando se proporciona un volumen mayor de datos. Así, en la sentencia de 6 de Octubre de 1999 de la Sala de lo Contencioso-administrativo del tribunal Superior de Justicia de Madrid, Sección 8ª[37], se exonera de responsabilidad a una empresa que había recabado datos con fines de publicidad del repertorio electrónico Ibertex de Telefónica (el afectado sostenía que los datos utilizados con fines de publicidad directa excedían de los mencionados en la guía ordinaria, como manifestaba la empresa demandada, lo que implicaba tratamiento y cesión de datos inconsentidos). Lo que sorprende es que en la misma sentencia se menciona que en la citada base de datos se recogen, entre otros, datos como la profesión o actividad, además de los diferentes datos que especifican la dirección. Debemos entender que respecto del dato de la profesión, se ha obtenido previo consentimiento, porque, de lo contrario, no entendemos que tal circunstancia no se haya examinado por la Agencia de protección de datos, que aparece en el caso como órgano sancionador, ni por el Tribunal que resuelve, al menos a mayor abundamiento.

Una novedad respecto del almacenamiento de la información sobre números de teléfono, ha sido la aparición de los repertorios electrónicos. Se trata de unas bases de datos sobre dicha información, a las cuales se puede acceder libremente por cualquier usuario de la red. En principio, la diferencia de soporte no implica mayores problemas que los derivados de las guías tradicionales. De hecho, la regulación sobre estos directorios es compartida con las anteriores, según se deduce de la legislación antes citada. Sin embargo, la digitalización de la información permite que se pueda almacenar toda la información que contienen con suma facilidad. Tal hecho ha desatado el interés comercial por aquéllos[38]. Nos interesa esta cuestión porque pone de relieve que, dadas las circunstancias, no parecía necesaria la creación del Censo promocional por la LOPD, según se vio en otro Capítulo, pues los intereses publicitarios se satisfacen plenamente a través de estos repertorios.

En resumen, el régimen de inclusión de los datos personales en las guías telefónicas permite la misma sin necesidad de consentimiento por parte de los abonados, sin perjuicio de la posibilidad de exclusión voluntaria de los mismos. Como vemos, se trata de una solución que admite un grado "medio" de voluntad (lo que, en terminología anglosajona, se conoce como *opt out*), pues no se exige la misma en el momento inicial para la inclusión, sino que permite la voluntad negativa en un momento posterior. En la práctica, tal régimen se traduce en la aparición generalizada

---

[37] Repertorio de Jurisprudencia Aranzadi. Marginal RJCA 1999/4747. Número 607/1999.

[38] PINET, MARCEL. *Datos públicos o datos a los que puede acceder el público y protección de datos. XX Conferencia de protección de datos.* Agencia de Protección de Datos, 1998.

de los datos de los abonados dada su inactividad, cuando no su ignorancia. Este régimen satisface más, de hecho, a los operadores que a los abonados.

Ahora bien, la manifestación de la voluntad contraria a la inclusión de los datos en las guías no requiere ser reiterada en cada incidencia que se produzca con relación al contrato de línea con la operadora. Solamente será necesaria una manifestación cuando se produzca un cambio de dicha voluntad, como se afirma en la sentencia de la Audiencia Nacional (Sala de lo contencioso-administrativo, sección 1ª) de 19 de Noviembre de 2003.

La regulación sobre guías puede, no obstante, sufrir un profundo cambio, en relación con la participación de la voluntad de los abonados. En efecto, el artículo 12 de la Directiva 2002/58/CE, de del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[39], adopta otra posición en relación con esta cuestión. En la Exposición de Motivos de la Propuesta de Directiva de12 de Julio de 2000 ya se advertía que, si bien tradicionalmente las guías contenían los datos de los abonados, sin perjuicio de la posibilidad de excluirse, esgrimiendo razones de interés público y de prestación del servicio universal, sin embargo hoy día han surgido nuevas circunstancias que exigen replantearse tal panorama. Continúa afirmando la Exposición que, en los casos de telefonía móvil y correo electrónico, lo normal es precisamente que sus titulares oculten tal información, a lo cual se une la dificultad de los operadores de mantener unas guías de estos servicios actualizadas, como se dice más adelante. Así, concluye que es necesario modificar la regulación existente para exigir el consentimiento de los abonados. En este sentido, el artículo 12 de la Directiva 2002/58/CE establece lo siguiente:

Guías de abonados.

1. Los Estados miembros velarán por que se informe gratuitamente a los abonados antes de ser incluidos en las guías acerca de los fines de las guías de los abonados, impresas o electrónicas, disponibles al público o accesibles a través de servicios de información sobre las mismas, en las que puedan incluirse sus datos personales, así como de cualquier otra posibilidad de uso basada en funciones de búsqueda incorporadas en las versiones electrónicas de la guía.

2. Los Estados miembros velarán por que los abonados tengan oportunidad de decidir si sus datos personales figuran en las guías públicas, y en su caso cuáles de ellos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su suministrador, y de comprobar, corregir o suprimir tales datos. La no inclusión en una guía

[39] DO L 201, 31.7.2002.

pública de abonados, así como la comprobación, corrección o supresión de datos personales de una guía, no deberán dar lugar al cobro de cantidad alguna.

3. Los Estados miembros podrán exigir que para cualquier finalidad de un guía pública distinta de la búsqueda de datos de contacto de personas a partir de su nombre y, si resulta necesario, de un mínimo de otros identificadores, se recabe el consentimiento específico de los abonados.

4. Los apartados 1 y 2 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a su inclusión en las guías públicas.

Junto con la Propuesta del año 2000 de la mencionada Directiva, la Comisión presentó un documento justificativo de las soluciones adoptadas en aquélla. En el mismo se aclaraba que se trata de un artículo simplificado y no se incluía supresión de la posibilidad de cobrar por el derecho a ser excluido de una guía; tiene en cuenta los nuevos servicios de comunicaciones electrónicas y los nuevos tipos de servicios de guía[40].

En primer lugar, la Directiva 2002/58/CE trató de reforzar la posición de los abonados. En este sentido, se exige a los responsables de las guías un deber de información, que pretende compensar la ausencia de consentimiento inequívoco de aquéllos. Además, se evita el carácter disuasorio que supondría el cobro de este servicio.

Estamos plenamente de acuerdo con el legislador europeo, pues entendemos que en los momentos actuales no se observan las razones que justifican la inclusión inconsentida en las guías. Hoy día, el uso cada vez mayor de los teléfonos móviles y la dificultad de configurar listados de los números de éstos, no encaja con la función de interés público de las guías. Los informes de resultados económicos sobre telefonía reflejan un gran crecimiento del uso de los terminales móviles y el estancamiento de la facturación en la telefonía fija, la cual pueda mantenerse, quizás, por la necesidad de tener una línea para la conexión a Internet. Así y con la progresiva equiparación de las tarifas de telefonía móvil y fija, es probable que la primera termine por ser el medio preponderante de comunicación por voz.

Por lo tanto, la evolución no aconseja el mantenimiento de una regulación que, sin proteger los derechos de los afectados, tampoco se justificaría, en

---

[40] *Propuesta de Directiva del Parlamento europeo y del Consejo relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*. Bruselas, 12-7-2000. COM (2000) 385 final. El texto íntegro de la Propuesta se puede obtener mediante su descarga en http://www.europa.eu.int/

épocas relativamente cercanas, por la satisfacción de interés general alguno[41]. Por otra parte, es muy positiva la extensión de la voluntad de los afectados al volumen de datos que se va a publicar en la guía, pues, como hemos visto anteriormente, la estricta finalidad de favorecer las comunicaciones elimina la necesidad de incluir algunos de los que actualmente se recogen en las guías.

Por otra parte, como ha previsto algún autor, la elaboración de las guías telefónicas no es ya labor propia de un operador, sino que la normativa prevé la posibilidad de que aquéllas se realicen por los diferentes operadores concurrentes: el artículo 38.6 de la LGT establece que

> *Le elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías. A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas la solicitudes razonables de suministro de información pertinente para la prestación de servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.*

Esta posibilidad implica la captación de los datos de los abonados por parte de los nuevos operadores, lo que supone cesión de los mismos, primero a la Comisión del mercado de las Telecomunicaciones y después de ésta a los demás operadores. Según Aspas Aspas[42], tal cesión requiere consentimiento inicial de los afectados o abonados en el contrato, pues no está prevista en la Ley, ni proceden éstos de fuentes accesibles al público ni se requiere la misma para el control, desarrollo o ejecución de un contrato entre responsable y afectado; supuestos éstos en los que el

---

[41] La Propuesta de Directiva motivó la actuación del "Grupo de Trabajo", el cual ha emitido el dictamen 7/2000, adoptado el 2 de Noviembre, sobre la citada Propuesta. En relación con el artículo 12 de la misma, el dictamen reproducía parte de los argumentos ya utilizados en otros dictámenes (concretamente, el dictamen 5/2000, al que aludimos en páginas posteriores). Básicamente, se afirma que, de acuerdo con la Propuesta, debe exigirse la voluntad de los abonados para figurar o no en las guías y, en concreto, en las que permiten la búsqueda inversa. Además, ante la posibilidad de la edición por cualquiera de las guías, exige que se respeten las opciones de exclusión y demás inicialmente manifestadas por los abonados (lo cual parece que no se cumple en algunos casos), para lo cual se requiere la previa información a los mismos sobre estas posibilidades. Finalmente, entiende el Grupo de Trabajo que, en los casos de cesión de los datos por soporte CD ROM, deben arbitrarse los medios técnicos que impidan la utilización de datos desfasados sobre las opciones que los abonados eligieron.

[42] ASPAS ASPAS, JOSE MANUEL. *Op. cit.* Pág. 1548.

artículo 11 justifica la cesión inconsentida. No obstante, el citado autor parte de la consideración de que los datos cedidos por las compañías son aquéllos a cuyo conocimiento han accedido por medio del contrato de suministro celebrado. Sin embargo, el operador dominante podría ceder exclusivamente los datos que obran en las guías telefónicas previamente realizadas, para lo que no requeriría consentimiento alguno. No obstante, hemos de reconocer que el supuesto normal será el de la cesión de datos provenientes de los contratos (única posibilidad de que gozan, en un primer momento, los operadores no dominantes), por lo que efectivamente es necesario el consentimiento.

En cualquier caso, hoy día existen posibilidades técnicas para captar los datos de las guías existentes, que recordemos son fuentes accesibles al público, de manera que un operador podría completar éstas con los datos de sus abonados obtenidos por la relación contractual. Posibilidad ésta que, sin embargo, no podría utilizar el operador dominante, pues no tiene otra forma de obtener los datos de los abonados a otras compañías que mediante la cesión. Para conseguir una idéntica posición de los operadores, parece conveniente la solución de las cesiones a través del organismo regulador de las telecomunicaciones. Por último, debemos recordar que tal organismo solamente cederá los datos necesarios para la elaboración de las guías, que, a nuestro entender, coinciden con los requeridos para facilitar las comunicaciones, con independencia de cuáles sean los datos personales que los operadores previamente cedan a la citada Comisión.

La mayoría de las cuestiones anteriormente planteadas han sido reguladas recientemente. La Orden 711/2002, de 26 de Marzo, del Ministerio de Ciencia y Tecnología, regula las condiciones aplicables a las guías telefónicas y al servicio de consulta telefónica sobre números de abonado. Establece esta norma, en su punto tercero, lo siguiente:

> *1. Los datos personales que podrán obtenerse a través de las guías telefónicas y de los servicios de consulta sobre número de abonado se limitarán a los que sean estrictamente necesarios para identificar a un abonado concreto. A estos efectos, las entidades que deseen elaborar guías telefónicas y los proveedores de los servicios de consulta sobre números de abonado únicamente podrán utilizar, en sus bases de datos, la siguiente información relativa a cada abonado:*
>
> *a) Nombre y apellidos, o razón social;*
> *b) Número(s) de abonados(s);*
> *c) Dirección postal del domicilio, exceptuando piso, letra y escalera;*
> d) *Terminal específico que deseen declarar, en su caso.*
>
> *2. No obstante, adicionalmente a lo dispuesto en el número anterior, los proveedores de servicios de consulta sobre números de abonado podrán utilizar otros datos personales de los abonados siempre que éstos hayan dado*

su consentimiento inequívoco. A estos efectos, se entenderá que existe consentimiento inequívoco de un abonado de un servicio de telecomunicaciones disponible al público cuando éste se haya dirigido a su operador o proveedor por escrito solicitándole que amplíe sus datos personales que figuran en la guía o servicio e directorio, al proveedor del servicio de consulta sobre números de abonados solicitándole que amplíe sus datos personales sobre los que se pueda facilitar información. También se producirá cuando el operador o proveedor solicite al abonado su consentimiento y éste les responda fehacientemente en el plazo de un mes dando su aceptación.

3. Se requerirá el consentimiento expreso de los abonados del servicio telefónico móvil disponible al público y de los abonados de los servicios de inteligencia de red para poder utilizar la información a que se refiere el punto 1 de este apartado.

Además, cuando los usuarios no sean titulares de un contrato de abono, tales como usuarios adicionales al titular del contrato, propietarios de tarjetas de pago previo de servicios de telecomunicaciones, sólo se podrá utilizar dicha información cuando los interesados hayan manifestado su deseo de figurar en las guías o en los servicios de consulta sobre números de abonado. En el caso de usuarios adicionales al titular del contrato, se requerirá el consentimiento previo de éste.

4. Los usuarios de servicios de telecomunicaciones disponibles al público podrán exigir a los operadores y proveedores que se les excluya de las guías telefónicas o de los servicios de consulta telefónica sobre números de abonado, que se indique que sus datos personales no pueden utilizarse para fines de venta directa, que se omita, total o parcialmente, su dirección u otros datos personales, o que se enmienden los errores existentes en sus datos personales. A estos efectos, se entenderá que las demandas de que los abonados realicen en relación con las guías telefónicas son extensibles a los servicios de consulta sobre números de abonado, salvo manifestación en contra.

Los operadores que presten el servicio telefónico disponible al público especificarán en sus correspondientes contratos de abono la forma en que podrán ejercer el derecho que se regula en este punto. A estos efectos, el abonado comunicará al operador su petición con la acreditación de recepción de dicha comunicación.

Los operadores y proveedores deberán proporcionar las posibilidades de exclusión a las que se refiere este punto gratuitamente a los abonados.

Por su parte, la Disposición adicional 1ª dispone que en las guías telefónicas incluidas en el servicio universal de telecomunicaciones deberán figurar los mismos datos mencionados en el punto tercero de la Orden, ya reseñado. Según el apartado 2º de esta disposición, la forma en que deberán figurar los datos mencionados es la siguiente:

> *2. Los datos estarán relacionados por orden alfabético del primer apellido o razón social. Después del primer apellido se reflejará completo el segundo, seguido tras una coma, del nombre propio o de sus iniciales. Asociado a cada número figurará además la dirección del abonado, sin especificación del piso o letra y, en su caso, un identificador del tipo de terminal (teléfono normal, fax, RDSI, videoconferencia, telefonía móvil, telefonía de texto para sordos, etc.). Asimismo, los abonados podrán exigir, a través de sus operadores, que se omita de su dirección el número de portal, así como que se indique que sus datos no pueden utilizarse para fines de venta directa.*

Como se puede comprobar, esta normativa continúa manteniendo la misma posición respecto de la información que se proporciona por las guías, así como de la no necesidad de consentimiento para la inclusión de los datos de los abonados referidos en el apartado 1º. En efecto, mantiene la posibilidad de los abonados de excluirse de las mismas: la opción *op-out*. Tal solución es contraria a las intenciones manifestadas ya por el legislador comunitario en la Propuesta de reforma de la Directiva 97/66, así como por el Grupo de trabajo del artículo 29. De ahí, que no entendamos el tenor de los preceptos de la Orden reproducidos. Por su parte, el artículo 12.2 de la Directiva 2002/58 mantiene la línea de los citados precedentes. Dispone aquél que

> *2. Los Estados miembros velarán por que los abonados tengan la oportunidad de decidir si sus datos personales figuran en una guía pública, y en su caso cuáles de ellos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor, y de comprobar, corregir o suprimir tales datos. La no inclusión en una guía pública de abonados, así como la comprobación, corrección o supresión de tales datos personales en la guía, no deberán dar lugar al coro de cantidad alguna.*

Ya sabemos que la "decisión" de la inclusión en las guías puede manifestarse de forma tácita. Sin embargo, tanto los precedentes citados como la falta de expresión normativa respecto del derecho a negarse a figurar en aquéllas, nos hace sostener lo contrario. Por otra parte, si los abonados deben manifestar pueden o no figurar, se requiere en tal caso forma expresa, lo cual parece extenderse a la mera voluntad de figurar.

Por otra parte, la Orden ministerial tiene el acierto de incluir una serie de novedades relativas a otros servicios no contemplados por la normativa anterior. Nos referimos a los servicios de información telefónica, respecto de los cuales se adopta un régimen idéntico al de las guías. Además, se admite la prestación de información sobre números de teléfonos móviles, lo cual resulta contradictorio con las propuestas realizadas por los órganos de trabajo comunitarios. Es curioso observar como respecto de la información de los números de los teléfonos móviles se exige consentimiento expreso. No encontramos razón alguna que justifique un tratamiento tan diferenciado y favorable de los derechos de los abonados, respecto de los números

de telefonía fija. La misma solución se adopta respecto de aquellos supuestos de empleo de tarjetas prepago. Ello implica que el grado de protección de los datos de carácter personal se hace depender de las características técnicas del medio utilizado: lógicamente es imposible acoger a este tipo de abonados en una relación de los mismos, por la perentoriedad de los números adjudicados con estas tarjetas. Sin embargo de tal circunstancia, ello es contrario al principio general de la normativa comunitaria sobre la materia, que exige una regulación neutra desde el punto de vista técnico, que exige una equiparación del nivel de protección, cualesquiera que sean los medios empleados.

Respecto de las cesiones de datos de carácter personal de la Comisión del mercado de las telecomunicaciones a las entidades que pretendan elaborar guías telefónicas y a las que se estén habilitadas para prestar información telefónica, determina el apartado 1º del punto 15º:

> *La Comisión del mercado de las telecomunicaciones, previa petición, facilitará a las entidades que estén habilitadas para prestar el servicio de consulta telefónica sobre números de abonado la información actualizada que pueden utilizar en sus bases de datos, a la que se refiere el apartado 3ª. Igualmente, facilitará a las entidades que elaboren guías telefónicas que incluyan, al menos, los datos contenidos en la guía comprendida en el ámbito del servicio universal de telecomunicaciones la información que pueda figurar en éstas.*

Se contempla, en este caso, un supuesto de cesión, respecto del cual la Orden ministerial omite la necesidad de que concurra consentimiento de los abonados. En líneas anteriores hemos visto que existe algún autor que sostiene la necesidad, salvo supuestos excepcionales que encajan en el artículo 11.2 c) de la LOPD, de dicha voluntad. Igualmente, se ha sostenido que la plasmación de tal solución en una norma de rango reglamentario no puede servir de argumento suficiente para justificar la exoneración de consentimiento. No obstante, pudiera entenderse que el origen de los datos proporcionados a quienes desean elaborar guías procede, a su vez, de otra guía, la cual recibe la calificación de fuente accesible al público por el artículo 3 j) de la LOPD. Por lo tanto, se evitaría el obstáculo derivado de las exigencias de jerarquía normativa.

c. El problema de los directorios inversos.

El desarrollo de las nuevas tecnologías ha permitido la aparición de los llamados directorios electrónicos, mediante los cuales es posible realizar una consulta sobre un determinado número de teléfono a través de la red. Las ventajas que conllevan tales directorios radican en la agilidad de la consulta desde cualquier punto en que haya conexión, a la vez que permite averiguar números no propios del ámbito provincial, sino pertenecientes a zonas situadas más allá de tal circunscripción. Como hemos visto, la normativa establece que las guías telefónicas tendrán, como mínimo,

ámbito provincial. En la práctica esta es la fórmula utilizada para su confección, por lo que los directorios electrónicos tiene la ventaja de contener una información de mayor alcance.

No obstante, no son los repertorios ubicados en la red los que plantean problemas respecto de la protección de los datos de carácter personal. Su análisis jurídico se remite a aquél que se realice respecto de la protección de los datos que aparezcan en la red. En realidad pretendemos analizar un tipo de estos directorios: los denominados directorios inversos. Con tales términos se hace referencia a aquellos repertorios ubicados en algunas páginas o sitios de la red, en los que es posible acceder, no sólo a la información sobre el número contratado por un abonado y su dirección, sino que, de modo inverso, es posible teclear el número de teléfono y extraer quien es el abonado y su dirección. De esta forma, el dato que determina el conocimiento del resto no es el nombre y apellidos del abonado, sino el mero número de la línea telefónica.

Las posibilidades ofrecidas por las aplicaciones informáticas permiten la creación de las denominadas bases de datos relacionales, las cuales conectan todos los campos sobre un mismo sujeto entre sí (en este caso, los campos que aparecen son el nombre y apellidos, número y dirección), de manera que desde cualquiera de ellos se puede acceder al resto de la información sobre el mismo. Como ya se ha señalado, la evolución de los equipos y sistemas informáticos ha permitido que los datos se puedan digitalizar en aras de una mayor agilidad de tratamiento, lo cual se puede hacer mediante una sencilla operación de escaneo, posibilidad que está al alcance no sólo de los operadores telefónicos, sino de cualquier particular en su domicilio.

En España, como en otros tantos países, los directorios electrónicos han surgido de modo inesperado y en una situación de cierto vacío normativo[43]. El caso con mayor trascendencia pública, pues apareció en las noticias de una conocida televisión, es el de la página de Internet *Infobel.com*, ubicada en un servidor que tenía su sede en territorio belga. En dicho directorio se podía teclear un número de teléfono para que, a continuación, apareciera el nombre y apellidos del abonado y su dirección (a tal información se acompañaba un mapa de la población, para ubicar la dirección, pues el directorio tiene carácter internacional). Ante la sorpresa que tal información

[43] No obstante, ya se encontraban algunas referencias a la existencia de tales repertorios y a sus problemas. Por ejemplo, la Agencia Española de Protección de Datos ya aludía a los directorios inversos con ocasión del análisis de las guías electrónicas, en la Memoria de 1997.
La sofisticación en los sistemas de búsqueda y tratamiento de la información ha alcanzado límites inimaginables. Por ejemplo, la posibilidad de cruzar los datos del Censo electoral con los correspondientes de las guías telefónicas, mediante el empleo de un software ofrecido por la empresa británica UK Infodisk.

provocó, la Agencia Española de Protección de Datos inició una inspección sobre este sitio[44].

Marcel Pinet[45] señala que, si bien los directorios inversos muestran la misma información que las guías normales, sin embargo la posibilidad de conocer datos de carácter personal por el mero conocimiento del número de teléfono implica que es posible tener acceso a una información personal que el afectado quizás no quisiera prestar, además de que tal divulgación se hace sin que tenga conocimiento de tal posibilidad. Efectivamente, cuando un sujeto aparece en la guía normal, sabe que, cualquier persona que conoce sus datos de identificación y, más aún, su dirección, puede conocer su número de teléfono. Sin embargo, puede que se encuentre con la negativa de aquél, porque, como dice Pinet, se está prestando más información de aquélla de la que, en principio, se estaría dispuesto a proporcionar.

La posición de las legislaciones de nuestro entorno respecto de este problema no es única. En algunos países, como Alemania o Inglaterra, tales repertorios están prohibidos, mientras que en Francia se condiciona su admisión al conocimiento de los afectados y a la posibilidad de que se autoexcluyan. En España, la normativa sobre guías telefónicas no se pronuncia expresamente sobre esta cuestión. Sin embargo, nosotros entendemos que se puede deducir una solución. No obstante, en el seno de Unión Europea sí existe alguna inquietud respecto de esta cuestión, como se deduce de los trabajos realizados en distintos organismos de la misma. En concreto, el Grupo de Trabajo sobre la protección de Datos, ya mencionado anteriormente, realizó un dictamen sobre la materia: el Dictamen 5/2000, adoptado el 13 de Julio, sobre el uso de guías telefónicas públicas para servicios de búsqueda inversa o multicriterio (Guías inversas).

Según se deduce de este dictamen, la prestación del número de teléfono por parte del interesado, ya sea casual o voluntaria, puede implicar una serie de consecuencias no deseadas por el titular del número, pues puede proporcionar información, no sólo relativa a la identificación y dirección del sujeto, sino incluso de la profesión o empleo. Además, se amplían las posibilidades a partir del mero número telefónico, ya que el conocimiento de la factura permite conocer los nombres y direcciones de las personas con quienes se ha comunicado. Incluso, en algunos casos se proporcionan, no ya un elemento de ubicación de la dirección como los mapas, sino fotografías de las viviendas. Finalmente, el Grupo de Trabajo recuerda que estas posibilidades aumentan si tal información se conecta a la que figura en los registros públicos. Es decir, como ya señalaba algún autor y reconoce el informe, el conocimiento del número de teléfono permite conocer una cantidad de información cuyo titular no desea ni espera.

---

[44] Hasta la fecha, desconocemos si la Agencia Española de Protección de Datos ha llegado a conclusión alguna y ha adoptado, en tal sentido, alguna solución al respecto.

[45] PINET, MARCEL. *Op. cit.*.

Las guías telefónicas, cualquiera que sea su soporte, justifican su existencia por su finalidad de facilitar las comunicaciones, al proporcionar los números telefónicos de aquellas personas con quienes se desea comunicar. Desde este punto de vista, parece lógico admitir la licitud de las guías tradicionales, pues a partir de los datos de identificación del sujeto se conoce el número para contactar. Ahora bien, el fin que se consigue con los directorios inversos no es precisamente el manifestado. Cuando uno pretende llamar a alguien, ya lo conoce previamente, lo que no sabe es su número. De esta forma, resulta contrario a toda lógica de la comunicación que uno sepa el número telefónico, pero no conozca a quien pertenece, pues en este caso no puede tener una intención de comunicarse con tal persona ni conseguir tal pretensión. Nadie tecleará números de forma aleatoria para averiguar si pertenecen a aquél con quien desea comunicar.

Por lo tanto, los directorios inversos no sirven como medios de facilitar la comunicación, mientras que sí permiten conocer datos sobre personas con las que no se pretende tener tal comunicación. Es cierto que la normativa guarda silencio sobre esta cuestión, lo cual permitiría aparentemente adoptar una postura permisiva. Sin embargo, hemos de tener en cuenta que si se está regulando esta materia con ocasión de la protección de datos de carácter personal, la ampliación de la restricción del sentido de la norma se predica de los derechos de los afectados, no de las posibilidades de los instrumentos que puedan limitarlos o aminorarlos.

En alguna ocasión, el Grupo de trabajo del artículo 29 ha pretendido ver en estos directorios inversos un instrumento que puede satisfacer intereses legítimos, al conceptuarlo como una extensión de los medios de identificación de llamada y de quien la efectúa[46]. Sin embargo, no creemos que por dichas razones se posibilite el conocimiento de tales datos en supuestos no revestidos de dicha legitimidad. Para lograr tal fin, deben facilitarse otros medios menos traumáticos. La falta de la finalidad propia de las guías en el caso de estos directorios inversos, que justifica la consideración de las primeras como fuentes accesibles al público, priva a las mismas del mínimo grado de licitud. Además, si los datos que pueden figurar en la guía son los que permiten de modo estricto identificar al abonado, tal objetivo no se satisface con los métodos de búsqueda inversa, al desconocer previamente a la persona que se pretende identificar. Aunque la Agencia Española de Protección de Datos no se pronunció expresamente, sin embargo sí advertía indirectamente que el problema podría resolverse en el sentido apuntado.

---

[46] GRUPO DE TRABAJO DE PROTECCION DE DATOS PERSONALES DEL ARTICULO 29. *Dictamen 7/2000 sobre la Propuesta de la Comisión Europea de directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de Julio de 2000*. COM (2000) 385, de 2 de Noviembre de 2000. (5042/00/ES/Final).

Por otra parte, el problema originado por los directorios inversos es similar a la solicitud del nombre del abonado de un número de teléfono a los servicios de información telefónica, los cuales se negaban sistemáticamente a prestar dicha información. Aunque algunos autores entienden excesiva tal negativa[47], sin embargo parten de la premisa de que los directorios inversos satisfacen un interés legítimo de establecer una comunicación, cuando en realidad facilitan la consecución de otros muchos fines, indeseables algunos.

La opción anterior se refuerza si tenemos en cuenta que hoy día es posible identificar el número de llamada entrante, salvo que quien efectúa la llamada desactive tal servicio, lo cual no es muy común en la práctica. Ambas posibilidades se regulan en los artículos 69 y siguientes del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, por imperativo de la antigua Directiva 97/66. Así, es posible que, conociendo primero el número, se pueda después saber a quien pertenece. Desde un criterio de lógica sistemática, debemos pensar que si la norma permite evitar que el receptor pueda conocer el número desde el que se llama, mayor razón existirá para poder evitar que, conocido ese número, se pueda averiguar quien es el abonado y su dirección.

La Orden ministerial 711/2002, ya mencionada, acoge la solución propuesta en estas líneas. En efecto, el apartado 5 del punto tercero establece que

> *Los proveedores de servicios de consulta sobre números de abonado, y las guías telefónicas en formato electrónico, rechazarán las consultas que permitan obtener la identidad o el domicilio de un abonado a partir de su número de teléfono u otro recurso identificativo de abonados.*

Como se puede observar, la redacción de este precepto no deja lugar a dudas. Debe, además, tenerse en cuenta, que el mismo hace extensiva esta solución de forma expresa, a los directorios electrónicos que faciliten métodos de búsqueda inversa. Por todas estas razones, el régimen jurídico de las guías inversas no puede ser el mismo que el establecido respecto de las guías convencionales, puesto que la finalidad de unas y otras no son las mismas. Es decir, no se puede admitir su configuración sin más como fuentes accesibles al público, de manera que la aparición en estos directorios de los abonados se produzca de la misma manera que en las guías tradicionales. Por el contrario, la posibilidad de que tales repertorios contengan los datos de aquéllos no se puede amparar en la normativa que regula las segundas, pues la diferencia de fines impide el beneficio de su consideración, sin más, como fuentes accesibles al público. De ahí que las guías inversas requieran la habilitación proveniente de una legislación propia, que tenga en cuenta sus características, posibilidades y objetivos. Se trataría de adoptar una solución similar a la que la LOPD acoge sobre el Censo promocional, como regulación diferente de la general del Censo, contenida en la legislación electoral.

---

[47] CORRIPIO GIL-DELGADO, MARIA DE LOS REYES y MARROIG POL, LORENZO. *Op cit.* Pág. 246.

Ahora bien, aunque efectivamente el consentimiento del abonado actúa como factor legitimador del tratamiento de los datos, sin embargo es conveniente adoptar una regulación específica de este tipo de guías, que recoja un régimen especial sobre la materia, pues en la práctica el desconocimiento de la misma provoca que, en muchos casos, se puedan producir abusos derivados de dicha ignorancia. Se trataría de una solución similar a la que la LOPD ha adoptado sobre el Censo Promocional respecto de la regulación general sobre el Censo electoral, contenida en la LOREG. En este sentido, la Directiva 2002/58 ha colmado el vacío existente, incluyendo en su artículo 12.3 una regulación sobre las guías inversas. Dice este precepto:

> *3. Los Estados miembros podrán exigir que para cualquier finalidad de una guía pública distinta de la búsqueda de datos de contacto de personas a partir de su nombre y, si resulta necesario, de un mínimo de otros identificadores, se recabe el consentimiento específico de los interesados.*

La solución aportada por la normativa comunitaria conlleva varias ventajas. Por una parte, genera una regulación específica para una cuestión de la misma naturaleza, a lo que se debe añadir el beneficio que conlleva la publicidad normativa respecto de un problema cuyo conocimiento es escaso para la mayor parte de los abonados, evitando los posibles abusos derivados de la ignorancia. Pero el efecto más positivo de la Directiva es la solución adoptada para habilitar la inclusión de los datos de los abonados en las guías. Según aquélla, es necesario el consentimiento del abonado para incluir sus datos. El dictamen del Grupo de Trabajo señala que tal consentimiento debe ser inequívoco, específico y previamente informado (información sobre el uso de los datos en este tipo de guías, posibilidad de revocar el consentimiento y medidas técnicas que garantizan el adecuado uso de aquéllos). Parece lógico exigir la participación de la voluntad del abonado, pues el asentimiento de éste a figurar en las guías tradicionales no incluye, ni mucho menos, las posibilidades de los repertorios inversos[48]. Ahora bien, obsérvese que la Directiva no sólo hace referencia a las guías electrónicas o que permitan métodos de búsqueda inversa, sino que exige el consentimiento de los abonados y la especificación de los datos que desean figuren en las mismas para cualquier tipo de repertorio (artículo 12.1), como ya se ha señalado anteriormente. Para garantizar la prestación de una voluntad consciente, exige igualmente la previa información al abonado sobre los posibles usos que se puedan realizar con sus datos.

La problemática que plantean los mecanismos de búsqueda inversa de datos de carácter personal en la red se plantea, no solamente con relación a las guías telefónicas, sino también con cualquier otro tipo de ficheros con información personal variada. La unificación de datos de carácter personal en ficheros accesibles a través de

---

[48] Tal exigencia de consentimiento nos lleva a preguntarnos cuál es la causa por la que no se adoptó la misma solución cuando se reguló por la LOPD el Censo Promocional, pues, al igual que ocurre en el caso que nos ocupa, se trata de un supuesto en el que se alteran los fines iniciales del Censo electoral, aunque sea de forma indirecta.

la red se realiza hoy día con diferentes fines, en principio todos ellos legítimos. Así por ejemplo, la Administración utiliza Internet como un medio que facilita la consecución del principio de publicidad de los actos administrativos. En otros casos, se trata de favorecer el conocimiento y la investigación con la elaboración de bases de datos temáticas (bases de datos jurisprudenciales, doctrinales, de publicaciones científicas, etc.). Tales fines justifican por sí la utilización de la red para divulgar el contenido de los ficheros.

Sin embargo, hemos de pensar que, si bien tal divulgación satisface de modo efectivo dichos fines, a la vez se puede estar permitiendo la consecución de objetivos no tan loables. Por ejemplo, es posible que la publicación íntegra de las sentencias en Internet permita, dada la posibilidad de la búsqueda inversa, conocer todos las resoluciones judiciales pronunciadas sobre una misma persona, o conocer las sentencias dictadas por un Juez como ponente, o determinar el nivel de cumplimiento de las obligaciones dinerarias de un sujeto (lo cual puede resultar un prejuicio inaceptable, deducido de una sola sentencia condenatoria). La aparición en un edicto relativo a la ejecución de deudas tributarias, o referente al pago de un justiprecio, puede inducir en la toma de decisiones de crédito a las entidades bancarias en uno u otro sentido. Las posibilidades descritas aumentan si tenemos en cuenta que las diferentes bases de datos que se encuentran insertas en la red pueden ser cruzadas, con lo que la aparente insignificancia de la inclusión en unas bases, en principio desligadas entre sí, se convierte en un poderoso instrumento al servicio de diversos fines, no siempre legítimos, a la vez que en una amenaza real para la privacidad de los usuarios.

Aunque en la mayoría de los supuestos planteados (no en todos) el carácter público de las fuentes de procedencia de los datos provoca una disminución en el rigor del régimen jurídico aplicable, sin embargo existe una serie de normas que son de absoluta aplicación a todo supuesto de tratamiento de datos. En efecto, el consentimiento de los usuarios no será necesario para el tratamiento de los datos procedentes de fuentes accesibles al público, según se desprende del artículo 11 de la LOPD, sin embargo en ningún caso se puede evitar la aplicación de los principios generales contenidos en el artículo 4. Este precepto exige que los datos sean recogidos para la satisfacción de fines concretos y determinados, sin que se puedan tratar de forma incompatible con los iniciales propuestos en la recogida.

La amplitud de fines que potencialmente se pueden satisfacer mediante la publicación en Internet de los datos es incompatible con dicho principio de especificidad, pues resultan contradictorias con la exigencia de la determinación inicial tan amplias posibilidades, que otorgan a la búsqueda en red un carácter claramente genérico e, incluso, aleatorio. En este sentido, resulta imposible que se pueda recabar el consentimiento adecuado de los usuarios, dado que el mismo no se solicita para legitimar objetivos concretos, sino que se está solicitando un cheque en blanco. De la misma manera, es imposible cumplir el deber de información de los posteriores

tratamientos, pues se desconocen cuáles, en qué cantidad y por quiénes se pueden realizar los mismos.

En algún supuesto, por ejemplo en la publicación de actos administrativos, pudiera sostenerse que tales peligros existen en el supuesto de la publicidad fuera de la red, pero que la satisfacción de tal principio, tendente a la satisfacción de fines públicos, se coloca por encima de la protección de derechos individuales, aún con rango fundamental. Sin embargo, entendemos que en este caso se debe hacer una distinción, por sutil que parezca: no es lo mismo *publicado* que *público*. Mejor dicho, la publicación de los actos administrativos no permite sin más la utilización de los datos de carácter personal contenidos en los mismos para cualquier fin. No olvidamos que el acceso a los documentos administrativos requiere, por regla general, la concurrencia de un interés legítimo. Sin embargo, la mera publicación en red de tales ficheros no concuerda con tal exigencia. Por ello, sería conveniente arbitrar mecanismos técnicos que, además de satisfacer el principio de publicidad, permitieran el acceso a dicha información, impidiendo cualquier posibilidad de uso indiscriminado de la misma: exigir la concreción de los criterios de búsqueda, con el fin de eliminar posibilidad de una búsqueda genérica; evitar la copia total de la base de datos[49].

7. La identificación de la línea entrante y conectada.

Hoy día, entre los servicios de telefonía avanzada, existe la posibilidad de que quien recibe una llamada de teléfono conozca en un momento previo al comienzo de la comunicación, desde qué línea se está efectuando aquélla, al igual que quien hace la llamada pueda conocer el número de la línea a la que ha sido conectada su llamada. Se conocen estos supuestos como identificación de la línea llamante y de línea conectada respectivamente, según el artículo 38.3 f) y g) de la Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones, el artículo 69 del Reglamento de desarrollo del Título II de la Ley General de Telecomunicaciones y el artículo 8 de la Directiva 2002/58/CE. En muchos casos, tales facultades no supondrán agresión alguna a la privacidad del sujeto que llama, pues existe una relación personal que impide plantearse tal cuestión. Sin embargo, existen otros casos en los que el comunicante no desea necesariamente, y de manera justificada, que se conozca desde qué teléfono llama. En este sentido, la Directiva 2002/58 ha entendido que esta identificación puede suponer una vulneración de la Intimidad, según expresión de la misma, de las personas (Considerando 36, *sensu contrario*). De ahí, la preocupación ha obligado a la aparición de una regulación al respecto.

---

[49] Sobre estas cuestiones, GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Privacidad en Internet: enfoque comunitario integrado de la protección d e datos en línea* (21 de Noviembre de 2000). 5063/00/ES/FINAL. http://www.europa.eu.int/

A los efectos de este trabajo, nos debemos plantear si la identificación de ambas líneas supone o no un supuesto de cesión de datos de carácter personal. Según el artículo 69.1 del Reglamento,

> *Lo establecido en este capítulo será de aplicación a los operadores que, de conformidad con lo establecido en la Orden reguladora de las licencias individuales y en el artículo 40 de este Reglamento, tengan la obligación de prestar servicios avanzados de telefonía con las facilidades de identificación de la línea llamante e identificación de línea conectada. Asimismo, deberán cumplir lo establecido en este capítulo los demás operadores que, sin estar obligados por la normativa anteriormente citada, presten voluntariamente dichos servicios.*

De este precepto se deduce claramente que tales facilidades se prestan por los operadores, es decir, éstos informan sobre dichos extremos. Sobre la base de la definición de cesión del artículo 3 de la LOPD, se entiende por tal la revelación de datos de carácter personal a persona distinta del afectado. En realidad, es esto precisamente lo que se está haciendo con la identificación de la línea llamante (en el caso de la identificación de la línea conectada no se plantea el problema, pues quien comunica sabe previamente el número al que llama). Podría entenderse que el sencillo número de la línea que se identifica no es, en realidad, un dato de carácter personal. Sin embargo, la también sencilla posibilidad de conocer la pertenencia de este número, mediante ficheros de búsqueda inversa, hace que se tenga que desechar tal posición. El número de teléfono permite, hoy día, identificar a un sujeto, al menos a los abonados. Pues bien, en estos casos el operador está cediendo información de tráfico a la parte de la comunicación distinta del abonado.

El régimen jurídico de este supuesto de cesión o comunicación de datos se contiene, como ya dijimos, en los artículos 69 y siguientes del Reglamento. De forma resumida, estos preceptos establecen lo siguiente: la identificación de la línea llamante se puede suprimir tanto por quien origina la llamada como por quien la recibe, excepto en los supuestos de llamadas a los servicios de urgencias. Tal supresión se puede hacer respecto de cada llamada, con el tecleo de un código (067)[50] o con carácter permanente para todas las llamadas. Por otra parte, el receptor podrá filtrar las llamadas en las que se haya suprimido previamente la identificación, con el fin de rechazar las mismas.

Como se puede deducir de lo anterior, el régimen de cesión o comunicación establecido no dista mucho de las reglas generales contenidas en el artículo 11 de la LOPD. En realidad, frente a la posibilidad del receptor de conocer previamente la línea entrante, está la de quien efectúa la llamada de eliminar tal

[50] La adopción de este código se realizó, por mandato del Reglamento, mediante la Resolución de la Secretaría General de Telecomunicaciones de 2 de Diciembre de 1998, por la que se atribuye el código "067" al servicio de supresión en origen, llamada a llamada, de identificación de línea llamante.

identificación. Por lo tanto, parece que depende de la voluntad de tal sujeto que se pueda conocer el número, es decir, se hace depender la cesión del consentimiento del afectado, en este caso el abonado que comunica. El artículo 69.3 obliga a los operadores a informar de forma individual a todos los abonados de estas facilidades, 15 días antes del inicio de las mismas. De esta forma, los abonados que no actúen para suprimir la identificación parecen prestar su consentimiento tácito a las mismas. No obstante, en estos casos las posibilidades de los abonados se han ampliado, dado que se les permite la posibilidad de eliminar la identificación en cualquier momento y de forma más ágil, para una llamada concreta o de modo general para todas, lo que, a su vez, facilita la revocación del consentimiento.

Ahora bien, el artículo 11.2 b) contiene un caso de excepción al consentimiento para las cesiones, cuando los datos cedidos estén contenidos en fuentes accesibles al público. Se podría entender, por tanto, que los números de teléfono identificados pueden ser cedidos sin necesidad de consentimiento, pues pueden estar contenidos en las guías telefónicas. Sin embargo, no entendemos entonces la necesidad de información por parte de los operadores a los abonados, ni mucho menos la posibilidad de éstos de suprimir la identificación, según vimos establece el Reglamento. La información mencionada no puede tener otro objetivo que permitir que los abonados puedan mostrar su voluntad conforme o no a estas facilidades. Sin embargo, a nuestro entender la posible contradicción sólo es aparente.

Quien tiene contratado el servicio de identificación no obtiene la información que, de modo general, se deduce de las guías telefónicas. De modo más preciso, no se obtiene la información en el mismo sentido que se proporciona por aquéllas. No se trata de conocer al abonado y, en función de esta información, acceder a su número y dirección, sino que la identificación facilita un método de búsqueda inversa, pues primero se conoce el número de la línea entrante. Sobre la base de la posición que sostuvimos con ocasión de los directorios inversos, entendemos que la identificación de la llamada entrante requiere el consentimiento de los abonados, pues el acceso a estos datos se contradice con la finalidad de la citada fuente accesible al público, requisito exigible al margen de la necesidad o no de consentimiento según el artículo 11.1 de la LOPD, lo cual impide la aplicación del régimen excepcional que establece en el artículo 11.2 b).

8. Los datos de carácter personal en las llamadas a números de emergencia.

La adecuada gestión de las urgencias requiere, entre otras medidas, la agilización de los procesos de tratamiento de la información necesaria para llevar a cabo aquéllas. En este sentido, la normativa de la Unión Europea y de los Estados miembros ha adoptado una serie de disposiciones tendentes a la normalización, que tiene alcance en todo el territorio de la Unión, de los números de atención de las urgencias, a la vez que ha sido necesario dotar a los gestores de la información recibida a través de esos números de una serie de facultades que modalizan o exceptúan las

reglas generales sobre protección de datos de carácter personal. Nos estamos refiriendo a la normativa reguladora del número telefónico 112.

Como ya se ha dicho, la introducción del número 112 como único número de urgencias europeo se adoptó por la Decisión de 21 de Julio de 1991 del Consejo de las Comunidades Europeas (hoy de la Unión), con fines de facilitar el acceso a las urgencias. En tal sentido, el artículo 75 del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, establece la obligatoriedad de eliminar la supresión de la identificación de la llamada entrante cuando la misma vaya dirigida a los teléfonos de urgencias. Tal precepto acoge las previsiones que la Directiva 97/66 establecía al respecto en el artículo 9 b). De la misma forma, el artículo 10.1 de la Directiva 2002/58 contiene la misma solución, incluyendo además el posible rastreo de llamadas malevolentes. Pues bien, en desarrollo de tales normas, se han promulgado en el Ordenamiento interno varias disposiciones.

Como dispone De Asís Roig, el artículo 75 del RD plantea un problema de jerarquía normativa, en tanto se emplea la norma reglamentaria para establecer regulaciones limitativas de derechos fundamentales protegidos, en principio, por la reserva de ley orgánica. No obstante, matiza el mismo autor tales afirmaciones, al entender, respecto de la eliminación de la supresión de identificación de llamada entrante, que la especial naturaleza de tales servicios pone en colisión bienes jurídicos de dimensión constitucional[51].

Concretamente, la regulación detallada sobre este número telefónico se realizó mediante el Real Decreto 903/1997, de 16 de Junio. Según el artículo 3.3 de este Decreto,

> …*Asimismo, dichos operadores* (se refiere a los operadores de redes y servicios) *facilitarán la identificación automática de la línea o zona geográfica desde donde se efectúen las llamadas* (hace referencia a los supuestos en los que llamada se haga desde un teléfono móvil) *al número telefónico 112, dentro de las posibilidades técnicas de la red y de acuerdo con la regulación que sobre las facilidades de presentación y limitación de la línea llamante se establece en la normativa nacional y comunitaria para salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación y persecución de delitos, la seguridad de la vida humana o razones de interés público.*
>
> *En todo caso, lo establecido en el párrafo anterior se entenderá sin prejuicio de las medidas que se adopten para garantizar el secreto de las comunicaciones, de acuerdo con lo establecido en el artículo 18.3 de la Constitución, y la protección de los datos personales, conforme a lo dispuesto en*

[51] ASIS ROIG, AGUSTIN E. *Protección de datos y derecho de las telecomunicaciones*. En *Régimen jurídico de Internet*. Colección derecho de las telecomunicaciones (Coord. CREMADES, JAVIER; FERNANDEZ-ORDOÑEZ, MIGUEL ANGEL; ILLESCAS ORTIZ, RAFAEL). Ed. La Ley. MADRID, 2002. Pág. 224-225.

la Ley Orgánica 5/1992, de 29 de Octubre, de regulación del tratamiento automatizado de datos de carácter personal, y en sus normas de desarrollo y disposiciones complementarias.

El desarrollo de lo dispuesto en el Decreto se recoge en la Orden del Ministerio de Fomento de 14 de Octubre de 1999, que regula las condiciones de suministro de información relevante para la prestación del servicio de atención de llamadas de urgencia a través del número 112. Tras reconocer nuevamente en su artículo 1º las posibilidades de identificación de línea llamante que establece el artículo 3 del citado Decreto, el artículo 2 dispone lo siguiente:

Los operadores obligados a los que se refiere el artículo 1, deberán facilitar a las Comunidades Autónomas, a las ciudades de Ceuta y Melilla o a las entidades prestatarias autorizadas que hayan asumido la prestación del servicio de llamadas de urgencias a través del número telefónico 112 (en adelante, entidades prestatarias), a petición de éstas, las correspondientes bases de datos que permitan relacionar e identificar el número de la línea llamante y la dirección (como mínimo, cuando estén disponibles: provincia, municipio, núcleo de población, código postal, calle, número de casa, planta y piso) o zona geográfica desde la que se efectúa la llamada, en el ámbito territorial de la competencia de aquellas.

En ambos casos, las mencionadas bases de datos contendrán, en la medida en que estén disponibles por parte de los operadores, el nombre, apellidos, documento nacional de identidad y dirección correspondiente al titular de la línea telefónica fija o móvil desde donde se efectúa la llamada…

En relación con el tratamiento de la información remitida por los operadores, dispone el artículo 4:

La cesión de datos personales referidos en el artículo 2 se entenderá amparada por la protección del interés vital del llamante, la seguridad pública y la protección del interesado o de los derechos y libertades de otras personas y quedará sometida a la legislación de protección de datos, Ley Orgánica 5/1992, de 29 de Octubre, de regulación del tratamiento automatizado de datos de carácter personal y su normativa de desarrollo. Dicha cesión de datos será utilizada, de manera exclusiva, como soporte para una más efectiva prestación de los servicios de atención de llamadas de urgencias a través del número 112 y será responsabilidad de la entidad prestataria el adecuado uso de los mencionados datos.

Los datos sobre ubicación geográfica de las estaciones bases de las redes públicas de telefonía móvil se utilizarán exclusivamente para la prestación del servicio de atención de llamadas de urgencia, no pudiéndose utilizar para otros fines ni cederse a terceros.

Como se reconoce en el artículo 4, el traspaso de la información mencionada en el artículo 2º a los destinatarios que el mismo cita, constituye un supuesto de cesión o comunicación de datos de carácter personal. Como se puede observar, los datos cedidos son todos aquéllos necesarios para la determinación exacta de la ubicación de la llamada. Parece lógico pensar que efectivamente el conocimiento de tal información permite tener más posibilidades de satisfacer de modo adecuado la urgencia. Así, la Agencia Española de Protección de Datos ha sostenido, en un informe sobre esta cuestión, que no se puede evitar la cesión de estos datos por los abonados que han solicitado a la operadora la supresión de la línea llamante, pues es prevalente el derecho a la integridad de las personas que la protección de los datos del llamante[52]. Ha entendido, además, que el consentimiento del abonado se exceptúa, incluso, cuando se recaben datos de salud, especialmente protegidos, puesto que los mismos se obtienen, precisamente, para solucionar una urgencia[53]. Claro está, la eliminación del derecho de supresión de la identificación, dado que se trata de una medida restrictiva, debe igualmente ser interpretada y aplicada de modo restrictivo a los supuesto precisados por la norma[54].

Ahora bien, si en la mayoría de los casos la llamada se efectúa desde un lugar cercano, cuando no el mismo, de aquél donde se requieren los servicios de urgencia, téngase en cuenta que no necesariamente ha de ser siempre así. Pensemos, por ejemplo, en aquellos casos en los que una persona comunica con el servicio de urgencias desde un móvil cuando conduce (lo cual es ilegal), de manera que puede que no se obtenga la determinación exacta del lugar del accidente. Por otra parte, la comunicación de los datos relativos a la identificación de la persona que ha efectuado la llamada puede resultar excesiva, cuando no está en presencia de quien requiere directamente la urgencia. Aunque tal exigencia puede eliminar posibles usos indebidos del teléfono de urgencia, sin embargo en la práctica muchos comunicantes no desean dar a conocer tales datos, pues entienden que han satisfecho el fin de auxilio con la llamada, pero a la vez prefieren preservar el anonimato.

Respecto de la cesión de los citados datos, está justificada la misma, según el artículo 4º, para proteger el interés vital del llamante, la seguridad pública y la protección del interesado o los derechos y libertades de otras personas. El sometimiento al principio de finalidad se recoge en la Orden Ministerial 711/2002, de 26 de Marzo, que limita los derechos de *todos los* abonados al uso legítimo que los

---

[52] Este y otros informes se pueden encontrar en la página de la Agencia, www.agpd.es. El mismo razonamiento se puede encontrar en CREMADES, JAVIER y RODRIGUEZ-ARANA, JAIME. *Comentarios a la Ley General de Telecomunicaciones (aprobada por Ley 32/2003, de 3 de Noviembre).* Colección derecho de las telecomunicaciones. La Ley. MADRID, 2004. Pág. 532.

[53] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Informe sobre teléfono de emergencia 112*. www.agpd.es.

[54] ASIS ROIG, AGUSTIN E. *Protección de datos y derecho de las telecomunicaciones*. En *Régimen jurídico de Internet*… Págs. 224-225.

prestadores de servicios de atención de urgencias hagan de los datos de aquéllos, como recuerda el informe de la Agencia Española de Protección de Datos, antes mencionado. No obstante, la redacción de este precepto no es muy afortunada. Por una parte, hemos de tener en cuenta que el llamante puede no coincidir, como de hecho ocurre en gran número de casos, con la persona que requiere la atención. Además, la mención del interesado tampoco cubre esta posibilidad, pues según la legislación de protección de datos es interesado aquél a quien se refieren los datos, en este caso, el abonado a la línea desde donde se hace la llamada. Quizás, la mención relativa a la protección de los derechos de otras personas sirva de fundamento para la cesión de los datos del abonado. De cualquier manera, hubiese sido preferible la adopción de una fórmula más correcta.

Las anteriores deficiencias se pueden salvar a la luz de la regulación contenida en el artículo 11 de la LOPD. Según la letra f) del párrafo 2º de este precepto, la cesión no requiere consentimiento del afectado cuando la misma sea necesaria para solucionar una urgencia que requiera acceder a un fichero. En este sentido, la adecuada prestación del servicio de urgencias conlleva la necesidad de conocer ciertos datos sobre la llamada y quien la efectúa, si bien con las limitaciones y precisiones que anteriormente hemos señalado sobre la determinación correcta de aquélla. Debemos tener en cuenta que, por ejemplo, los datos que se pueden obtener en el caso de que la llamada se haya hecho desde un teléfono móvil, indican que lo que se pretende es obtener mayor información sobre el lugar más o menos exacto en el que se requiere la atención de una urgencia, pues, aunque los operadores gozan de los datos tendentes a la identificación y dirección del abonado, sin embargo no son éstos los que se solicitan. Igualmente, se justifica la cesión y posterior tratamiento de estos datos porque van destinados al cumplimiento de una misión de interés público o que sea inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, supuesto en el que no se requiere consentimiento de los afectados, como dispone el artículo 7 e) de la Directiva 95/46.

Por otra parte, resulta curioso observar como respecto de las comunicaciones móviles se establece la prohibición de poder ceder los datos obtenidos, mientras que se guarda absoluto silencio respecto de las comunicaciones efectuadas por teléfono fijo. La anterior diferencia presenta mayores problemas si tenemos en cuenta que los datos que la Orden ministerial permite obtener son más cuantiosos en el segundo caso. Se puede interpretar que la estricta finalidad a la que se deben destinar estos datos impide la posibilidad de cesiones. Sin embargo, esto no es del todo cierto. Quizás la justificación a esta diferencia se pueda encontrar en el hecho de que los comunicantes por teléfono móvil no gozan de la misma ubicación que quienes lo hacen desde un teléfono fijo, lo cual permite que los servicios de urgencia a los que se cedan, en su caso, estos datos, puedan recabar más información de éstos últimos a los fines de la urgencia. En cualquier caso, las posibilidades técnicas no

deberían servir de pretexto para justificar mayores o menores posibilidades de acceso y tratamiento de los datos[55].

Una cuestión que pudiere ocasionar algunas dudas es la relativa a la naturaleza de los datos que se ceden a las entidades que gestionan el servicio de los teléfonos de urgencias. Efectivamente, pudiera sostenerse que al establecerse con carácter obligatorio, entre otros, la identificación de la línea llamante, se está cediendo un dato de tráfico, para lo cual se exige, dado que los mismos forman parte del secreto de las comunicaciones, autorización judicial. Sin embargo, debemos tener en cuenta que el caso ahora estudiado no encaja dentro del supuesto general que se regula en el artículo 18.3 de la CE. Como ya dijimos con ocasión del examen del uso de los datos de tráfico y facturación para fines comerciales, la alteración de los fines que se pretenden con el uso de estos datos, modifica el régimen jurídico aplicable.

De esta forma, no se pretenden conocer estos datos con el objetivo de poder desentrañar aspectos de proceso de comunicación ya efectuado, sino que se fijan objetivos posteriores en el tiempo, en cuanto se pretende conseguir la prestación del servicio de urgencias del modo más satisfactorio posible. Téngase en cuenta, por otra parte, que en la práctica no resultaría operativa la exigencia de la intervención judicial, lo que provocaría que la satisfacción de fines de interés general quedara supeditada indebidamente a la protección de derechos individuales más allá de los límites propios de éstos.

---

[55] Aparte los casos de localización por motivos de atención de una emergencia, los datos de localización geográfica constituyen un tipo de datos de tráfico, en tanto que la señalización más o menos exacta en el espacio, se requiere para el establecimiento y conexión de las comunicaciones móviles. Por lo tanto será de aplicación el régimen, anteriormente analizado, de esta categoría de datos. Se definen estos datos, según el artículo 2 c) de la Directiva como *cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.*
Por otra parte, el artículo 9.1 de la Directiva 2002/58 establece, por otra parte, la necesidad de que concurra el consentimiento previo e informado del abonado o usuario para tratar los datos de localización que sean necesarios para la prestación de un servicio de valor añadido, salvo que dichos datos sean anónimos. La enmienda 17 de la Propuesta de reforma exigía, además, que estos servicios sólo podrán prestarse cuando medie la solicitud expresa del usuario. Así, los datos de localización pueden considerarse como datos de tráfico o como requeridos para la prestación de otros servicios, supuestos éstos que implican, respectivamente, la excepción o necesidad de consentimiento. Sobre estas cuestiones, CORRIPIO GIL-DELGADO, MARIA DE LOS REYES y MARROIG POL, LORENZO. *Op. cit.* Págs. 235-240. También, LOZA CORERA, MARIA. *Nueva legislación europea en materia de protección de datos.* Diario la Ley, núm. 5549. Año XXIII. 22 de Mayo de 2002. Pág. 2.

En desarrollo de sus competencias[56], la Comunidad de Madrid ha promulgado la Ley 25/1997, de 26 de Diciembre, de regulación del servicio de atención de urgencias 1-1-2. Esta Ley contiene una serie de preceptos reguladores de los ficheros de datos que el Centro de atención de urgencia posee como consecuencia de la prestación de sus servicios. Respecto de los mismos, hubiera sido deseable que su redacción fuere más clara y evitase la posibilidad de que fueran interpretados de forma contradictoria entre sí. Por un lado, establece el artículo 10, en sus párrafos 2º y 3º

> *5. Tales ficheros recogerán, entre otros, los datos de carácter personal de quien demande la prestación del servicio. Estos ficheros podrán recoger los datos relativos a la salud u otros protegidos por la legislación vigente, siempre que éstos sean voluntariamente cedidos por los interesados y resulten determinantes del modo en que deba prestarse la asistencia material requerida o atenderse la urgencia.*
>
> *6. Los datos contenidos en los ficheros a los que se refiere este artículo serán cancelados cuando finalice la actuación para determinar la*

---

[56] Con anterioridad a la citada norma, la Comunidad de Madrid hizo uso de sus competencias sobre regulación de los ficheros de datos de carácter personal de naturaleza pública mediante la Ley 13/1995, de 21 de Abril, de regulación del uso de la Informática en el Tratamiento de Datos personales por la Comunidad de Madrid. En el artículo 2.2 de la misma se establece que *las disposiciones de esta Ley son de aplicación a las Instituciones de la Comunidad de Madrid así como a la totalidad de los Organos, Organismos, Entes y Empresas integrantes de su Administración Pública.* Esta norma ha sido derogada por la Ley 8/2001, de 13 de Julio, de protección de datos de carácter personal en la Comunidad de Madrid. En el artículo 2.1 se establece que l*a Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por las Instituciones de la Comunidad de Madrid y por los Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, exceptuándose las sociedades mercantiles a que se refiere el artículo 2.2.c).1 de la Ley 1/1984, de 19 de enero, reguladora de la Administración Institucional de la Comunidad de Madrid.* El artículo 2.2 c) 1 de la Ley 1/1984 se refiere a l*as sociedades anónimas en cuyo capital sea mayoritaria, directa o indirectamente, la participación de la Comunidad o de sus Organismos Autónomos, salvo que por Ley de la Asamblea se autorice expresamente una menor participación.*
A este respecto, la citada Ley 25/1997, de 26 de Diciembre, de regulación del servicio de atención de urgencias 1-1-2, establece que tal servicio es público, sin determinación del sujeto concreto que presta tal servicio. No obstante, el Decreto 168/1996, de 15 de Noviembre, que regula la prestación del servicio de atención de urgencia a través de un número telefónico único, establece en su artículo 4 que la gestión se encomienda a una empresa pública en virtud de un convenio de colaboración entre la misma y la Comunidad de Madrid. En efecto, la Ley de presupuestos del año 2001 de la Comunidad de Madrid, por ejemplo, se refiere a dicha empresa como empresa pública con forma de Sociedad Anónima. En este sentido, la regulación de los ficheros de la misma puede realizarse por normativa autonómica, dado que se trata de normativa sobre ficheros públicos, lo cual puede ser competencia de las Comunidades Autónomas, no así la regulación de los ficheros privados. Cuestión diferente es si la configuración de los ficheros de esos entes y empresas deben considerarse públicos o no, pues en otras áreas de su actividad se rigen por normas de derecho privado.

actuación a la que, de manera mediata o inmediata, haya lugar, y en todo caso a petición del interesado.

A continuación, el artículo 11 dispone lo siguiente:

En la recogida y cesión de datos de carácter personal a los que se refiere el artículo anterior, deberá respetarse, con carácter general, lo previsto en la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal y en la Ley 13/1995, de 21 de Abril, de regulación del Uso de la Informática en el tratamiento de Datos Personales por la Comunidad de Madrid.

Sin perjuicio de lo establecido en el párrafo anterior, cuando la urgencia del caso lo requiera, no será necesario informar expresamente al interesado, ni recabar su consentimiento expreso para el tratamiento automatizado de los datos o para su cesión a las entidades encargadas de la prestación material de la asistencia o del servicio a que haya lugar.

En primer lugar, hemos de señalar que, en realidad, los datos solicitados que tengan el fin directo de la solución de la urgencia, serán relativos a la persona que requiera la atención, la cual no tiene que coincidir necesariamente con quien hace la llamada. Ahora bien, en este caso la normativa autonómica no hace referencia al abonado, por lo que podemos entender que los datos son relativos a la persona que realmente necesita los servicios, aunque puedan recabarse datos del llamante por motivos de identificación y ubicación. Resulta sorprendente la disposición del artículo 11, en la que se exonera de la información y consentimiento para tratar y ceder los datos cuando la urgencia del caso lo requiera. En realidad, creíamos que todas las llamadas se hacían por motivo de una urgencia real, de manera que no resultaba fácil determinar el grado de la misma en los momentos previos a la atención. Por lo tanto, entendíamos que, a priori, todos los casos eran urgencias que exigían la misma actuación, por lo que en todos ellos se permitía la exoneración de tales requisitos. La legislación sobre protección de datos exime de satisfacer dichos requisitos para el tratamiento y la cesión en los supuestos de actuación respecto de una urgencia, sin graduar la gravedad de la misma. Pues bien, la normativa autonómica establece, *sensu contrario*, para ciertos casos, la posibilidad de que el tratamiento y la cesión exijan información y consentimiento. Parece que tal solución resulta poco operativa, pues en la práctica será difícil que los servicios de atención telefónica puedan valorar adecuadamente esta circunstancia, por personas no peritas en determinadas materias (salud, desastres, riadas, etc.).

Por otra parte, la exigencia de cancelación de los datos cuando se haya concluido la actuación tendente a que los servicios de urgencia realicen las actividades necesarias, es decir, la comunicación y coordinación de los mismos, o cuando lo solicite el interesado, se exceptúa también cuando la urgencia del caso permita tratar los datos sin consentimiento ni información. Por las mismas razones antes apuntadas, creemos que en la mayoría de los casos la solución será la aplicación de la excepción,

por la dificultad de terminar la naturaleza de la urgencia. No obstante, creemos que resulta positivo que la norma distinga grados de urgencia, con el fin de evitar que la utilización genérica de este término permita sin más los tratamientos y cesiones desinformados e inconsentidos que, en algunas ocasiones en las que la urgencia no fuese de tal grado que justificase el acopio de información, pudieren no estar justificados.

9. Los datos de carácter personal tratados como consecuencia de las interconexiones.

La liberalización del mercado de las telecomunicaciones y la consiguiente aparición de distintos operadores, a los cuales se les debe facilitar el acceso adecuado a las redes existentes, con independencia de quienes sean sus titulares, obliga a la conexión entre aquéllas con el fin de proporcionar un servicio adecuado a los abonados y usuarios en general. A lo anterior se une la existencia de distintas redes, que exige su más perfecta coordinación e interconexión, según determinaba ya la Ley 31/1987, de 18 de Diciembre, de Ordenación de las Telecomunicaciones.

La interconexión resulta necesaria, por tanto, para facilitar el desarrollo de las actividades de los operadores, así como para posibilitar la comunicación entre los abonados y usuarios que hayan contratado o utilicen los medios facilitados por cualquiera de ellos. Claro está, la posibilidad de comunicaciones entre abonados de distintos operadores implica la necesidad de coordinar la información sobre los mismos y sus llamadas. En tales casos, se producen cesiones de datos de distinta naturaleza y, consecuentemente, se generan diversos tratamientos de los mismos. La Ley 11/1998, de 24 de Abril, General de Telecomunicaciones, establece en sus artículos 22 y siguientes la regulación de la interconexión de las redes. Se trata de una obligación que deberán facilitar los titulares de redes a todos los operadores que actúen sobre las mismas y resten servicios disponibles al público, cuando éstos lo soliciten. El Anexo de esta Ley contiene, entre otras, la definición de interconexión. Se entiende por tal,

> *La conexión física y funcional de las redes de telecomunicaciones utilizadas por el mismo o diferentes operadores, de manera que los usuarios puedan comunicarse entre sí o acceder a los servicios de los diferentes operadores. Estos servicios pueden ser suministrados por dichos operadores o por otros que tengan acceso a la red.*
>
> *La interconexión comprende, asimismo, los servicios de acceso a la red suministrados con el mismo fin, por los titulares de redes públicas de telecomunicaciones a los operadores de servicios telefónicos disponibles al público.*

Como consecuencia de la interconexión, pueden surgir problemas de determinación de la entidad que deberá facturar la llamada efectuada en la que se relacionen equipos conectados a unas u otras redes o cuando participen varios

operadores. A este respecto, el artículo 7.1 de la Orden del Ministerio de Fomento de 18 de Marzo de 1997, que determina las tarifas y condiciones de conexión a la red adscrita al servicio público de telefonía básica que explota el operador dominante para la prestación del servicio final y el servicio portador soporte del mismo, establece que

> *Cada llamada individual deberá ser facturada al usuario por una única entidad habilitada.*

A continuación, especifica cuál será la citada entidad, en función de los diferentes tipos de llamadas (metropolitanas, provinciales, interprovinciales, internacionales, etc.). También dispone el intercambio de información para la facturación de las llamadas en el artículo 7.3 y 4, según el cual

> *3. Las entidades habilitadas habrán de intercambiarse la información básica que resulte precisa para poder confeccionar las facturas a los usuarios. El detalle del procedimiento para dicho intercambio será acordado por las partes en un plazo máximo de dos meses desde la fecha en que el operador dominante reciba la solicitud de interconexión. Si en este plazo, ambas entidades no hubieran formalizado estos acuerdos, resolverá la Administración competente en un plazo máximo de un mes desde que fuese requerida al efecto, mediante una disposición de obligado cumplimiento…*
>
> 5. *Cada entidad habilitada habrá de girar una única factura al usuario, comprensiva de los importes correspondientes a los distintos servicios que a ella se le han solicitado.*

Al igual que sostuvimos con ocasión del análisis del tratamiento de los datos con fines de facturación, en este caso la finalidad estricta perseguida permite evitar la aplicación de la normativa sobre secreto de las comunicaciones. De esta forma, como se deduce del artículo 9 de la citada Orden ministerial, la gestión de tales datos se someterá a los principios de la protección de datos de carácter personal, en cuanto su finalidad no va destinada al conocimiento de los diferentes aspectos de la comunicación en sí misma, sino más bien a la satisfacción de fines de cobro. Obviamente, la cesión de los datos realizada por razones de facturación no requiere el consentimiento de los afectados, como se deduce, por otra parte, del carácter imperativo de la norma que establece esta cesión. Se trata de una norma que exonera el cumplimiento de tal requisito. La excepción a la necesidad de consentimiento en estos casos se apoya en el artículo 11.2 c), según el cual no deberá concurrir necesariamente aquel requisito cuando responsable y afectado sean partes de una relación jurídica, para cuya ejecución sea necesaria la cesión. No se puede discutir que la interconexión y facturación exige conocer los datos de abonados en los supuestos aquí estudiados.

Por motivos, no ya de cobro del servicio prestado, sino de la propia gestión de las interconexiones, el Anexo de la Orden ministerial contiene, entre otras, la Condición 5ª, en la cual se establece lo siguiente:

> … *Igualmente, las citadas entidades se comprometerán a proteger los datos personales de los usuarios de los servicios soportados por las interconexiones y que deban ser intercambiados entre ellas por motivos de gestión de la propia interconexión, así como a no hacer otro uso diferente de esos datos que el que justifica su intercambio.*

Las mismas razones que hemos apuntado respecto del tratamiento y cesión de los datos por motivos de facturación en líneas anteriores, se pueden ahora esgrimir en este caso. La posibilidad de realizar llamadas que requieran conexión de redes y de operadores conllevan la necesidad de tratar y ceder datos, es decir, tales actividades son presupuesto de la ejecución del contrato de los abonados con los operadores, circunstancia que permite prescindir del consentimiento, según el artículo 11.2 c) de la LOPD, como ya hemos señalado.

LOS DATOS DE CARACTER PERSONAL EN INTERNET.

1.- Introducción: el problema de la necesidad de una regulación específica de Internet.

El nivel de desarrollo que las telecomunicaciones han alcanzado hoy día no hubiera sido posible sin la aparición y aplicación de los medios informáticos. Si bien en los primeros momentos de este proceso se observaba una colaboración de los segundos en la mejora de aquéllas, con una nítida separación entre ambas áreas, sin embargo se tiende paulatinamente a la plena fusión, de manera que la telemática terminará por convertirse finalmente, en la comunicación por excelencia. En un futuro próximo, las más variadas comunicaciones no se realizarán por la telefonía convencional, sino que se utilizará Internet para estar conectado con el mundo de forma generalizada: relaciones con la Administración, adquisición de productos y servicios, gestión doméstica desde lugares remotos (por ejemplo, la puesta en marcha del microondas o de la lavadora), conversaciones en las que los interlocutores se observan entre sí, telefonía por Internet. Todas estas aplicaciones, actualmente utilizadas por número mas o menos mínimo de usuarios, constituirán más adelante el medio de comunicación ordinario. Se tiende, por tanto, a la desaparición de las formas tradicionales.

No obstante lo anterior, en nuestros días los diferentes medios conviven juntos. La novedad que implica Internet conlleva la escasez normativa al respecto. De esta forma, las diferentes cuestiones jurídicas que surgían respecto de aquella se solventan a la luz de la legislación de telecomunicaciones. No se puede negar la analogía existente entre telecomunicaciones en general e Internet. Se trata de formas de comunicación que, básicamente, circulan o se llevan a cabo por los mismos cauces. En efecto, el acto de comunicación en Internet se realiza a través de la línea telefónica, de manera que el usuario efectúa una "llamada" al servidor (como se puede observar, se continúa utilizando la terminología tradicional), que le conecta con el sitio[57] concreto. La diferencia estriba en la forma de circulación de la información: por conmutación de paquetes en el caso de Internet y por conmutación de circuitos en la comunicación telefónica tradicional. Por otra parte, los operadores suelen ser los mismos, siquiera mediante la creación de divisiones separadas según se trate de unas u otra, lo cual permite deducir, de nuevo, la cercanía señalada. Ambos factores, la falta de una regulación propia ante la novedad del fenómeno y las similitudes entre ambos medios, han supuesto la solución normativa antes apuntada.

---

[57] En este trabajo vamos a utilizar de forma indistinta los términos sitio web y página web. En realidad se trata de realidades diferentes, pues los sitios son lugares, por decirlo de alguna manera, en los que se albergan varias páginas. No obstante, a los efectos de la protección de datos de carácter personal resulta indiferente hacer una u otra alusión.

Quizás todos los argumentos anteriores y alguno más, justifiquen la existencia de una regulación unificada. Ahora bien, el factor que determina la necesidad de un régimen jurídico propio no es sólo la existencia de notas diferenciales sin más, sino que las mismas impliquen una sustancia exclusiva y diferente, propia de la institución que se pretende regular, la cual dote de una fisonomía particular a ésta última. ¿Concurren en Internet circunstancias que incidan en la necesidad de llevar a cabo un tratamiento jurídico separado de las telecomunicaciones en general?. Concretamente, nos referimos a la justificación de una regulación propia de protección de datos en el ámbito de Internet.

Efectivamente, Internet presenta una serie de especialidades respecto de los demás modos de telecomunicación que nos inducen a coincidir con quienes sostienen la conveniencia de una regulación separada, al menos en algunas cuestiones que se plantean exclusivamente en aquélla. La convergencia de la utilización de sistemas de comunicación y de herramientas informáticas, elementos ambos que permiten conjugar la velocidad de transmisión con las enormes posibilidades de gestión de la información, proporciona mayores posibilidades de tratamiento de datos de carácter personal, a la vez que aumenta las dificultades de control de los usuarios en la recogida y tratamiento de sus datos[58]. Tal conjunción ha dado lugar a la aparición de nuevos problemas que no se planteaban en relación con el uso de los mecanismos tradicionales de comunicación. Como no puede ser de otra manera, las mayores posibilidades de uso que ofrece Internet conllevan esta consecuencia. Cuestiones como la problemática de las *cookies* u otros medios de tratamiento invisible de datos no se plantean en las comunicaciones por telefonía vocal, por ejemplo. Es lógico, por tanto, que la legislación existente no aporte soluciones concretas para solventar problemas que no estaban en la mente del legislador. Según Castro Rey, uno de los mayores peligros que genera Internet respecto de la protección de datos de carácter personal radica en las enormes posibilidades de tratamiento de la información que se derivan de su configuración. En efecto, a diferencia de lo que ocurre con la telefonía tradicional, en la que cada terminal tiene detrás un ser humano, en Internet, cada nodo es un ordenador, con lo que las posibilidades de procesamiento son indefinidas[59].

---

[58] A este respecto, resulta sintomático el caso del médico de Mitterrand, Gubler. Tras el fallecimiento del Presidente de la República Francesa, Gubler publicó un libro relativo a las vivencias con el personaje político. Dicha publicación fue secuestrada judicialmente a solicitud de los familiares, por entender que la misma vulneraba el deber de secreto. Sin embargo, ya se habían vendido varios miles de ejemplares, uno de los cuales se ofreció en Internet. Así, se multiplicó la divulgación, sin que el empleo de un medio tradicional como el secuestro judicial, pudiera evitarlo. Se observa, así, la inadecuación de la normativa existente a la resolución de los problemas jurídicos derivados de Internet.

[59] CASTRO REY, JOSE LUIS. *Internet y la protección de datos de carácter personal en España.* Agencia Española de protección de datos, 1996. Pág. 13.

Tampoco se debe olvidar que la arquitectura de Internet proporciona la mayor de las divulgaciones posibles de la información que se incluya en aquélla. En este sentido, las posibilidades de conocimiento de los datos personales que se generen y circulen por la red son innumerables, lo cual conlleva un enorme riesgo para el control de la información personal. De ahí que sea necesaria la adopción de medidas que traten de evitar estos posibles perjuicios. En algunos casos, se han adoptado soluciones cualificadas por razón del medio de difusión, por razón de la particular naturaleza de Internet. Por ejemplo, la CNIL francesa (Commition Nationelle de la Informatique et des libertés) exigió el consentimiento expreso de las personas afectadas por la publicación de sus datos en la red. Entendía este organismo que la posibilidad de transferencia de los datos a países que no poseen una legislación protectora de la información personal, exige la adopción de soluciones específicas, por razón de la particularidad del *recurso* empleado[60]. Todo ello a pesar de que, como en el caso de la LOPD española (artículo 7), el artículo 31 de la Ley francesa nº 78-17 de 6 de Enero de 1978, sobre protección de la información personal, reserve esta forma de consentimiento para el tratamiento de los datos denominados sensibles.

A lo anterior debemos añadir una serie de características que, si bien implican grandes beneficios que justifican el enorme auge adquirido por Internet, sin embargo suponen simultáneamente la existencia de potenciales peligros para la protección de datos de carácter personal, como afirma Corripio Gil-Delgado[61]. Por una parte, una de las notas definitorias de Internet es su alto grado de interactividad. Internet es el medio interactivo por excelencia. Si a esto unimos la ausencia de intervención personal directa, la consecuencia es la utilización despreocupada de Internet. Sin embargo, como veremos más adelante, la conclusión no puede más errónea, por cuanto la utilización de los potentes sistemas informáticos comporta mayores posibilidades de control. Como se dice comúnmente, el uso de Internet por los usuarios deja rastro.

Otra circunstancia que agrava la labor de protección de datos es la inseguridad de la red. La dificultad en la protección de los contenidos o informaciones que circulan por Internet es elevada, ante la popularización del uso de los medios informáticos, que ha posibilitado que la realización de actos ilícitos haya tenido un aumento exponencial (sistemas, lenguajes, etc). Se debe tener en cuanta que la seguridad ha ido disminuyendo a medida que se ha incrementado el nivel técnico, pues en épocas anteriores la falta de mecanismos fiables de tratamiento de la información

---

[60] *Deliberations de la CNIL du 7 Novembre 1995 (nº 95-131 et nº 95-132) sur la demande de difusión de fichiers d´informations nominatives via l´Internet par deux instituts publics*. Sobre estas deliberaciones, BENSOUSSAN, ALAIN. *Internet. Aspects juridiques.* Ed. Hermès. PARIS, 1998. Págs. 171-172.

[61] CORRIPIO GIL-DELGADO, MARIA DE LOS REYES. *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet.* Agencia Española de Protección de Datos. Premio protección de datos personales, IV edición. 2000, MADRID.

evitaba mayores injerencias[62]. A la dificultad técnica para eliminar la inseguridad se une la inevitable lentitud de la protección normativa, sobre todo ante la celeridad de la evolución del fenómeno en cuestión.

Finalmente, otra característica que impide una solución normativa adecuada en la extraterritorialidad de Internet. Si bien los instrumentos internacionales y la regulación privada permiten disminuir el problema, sin embargo no eliminan del todo la existencia de vacíos, siquiera temporales. En este sentido, el Grupo de Trabajo del artículo 29 ha tratado de minimizar los problemas derivados de la extraterritorialidad, mediante la determinación de los puntos de conexión con la normativa comunitaria. Concretamente, el Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE (aprobado el 30 de Mayo de 2002)[63], estableció una serie de reglas respecto de los diferentes instrumentos de recogida y tratamiento de datos en la red. En primer lugar, dispuso el Grupo de Trabajo que la información recogida mediante la implantación de cookies, aplicaciones *javascript* o programas espía en los equipos de lo usuarios pertenecientes a Estados miembros, se rigen por el derecho del Estado donde se encuentre el equipo. También se exige que se proporcione a los usuarios información similar a la establecida para los responsables de los ficheros que se encuentran en territorio de la Unión Europea. Claro está, conseguir estos objetivos requiere la sensibilización de todos los sectores implicados y la participación activa de las autoridades de control.

No obstante, hemos de recordar que la intención de los creadores de Internet era precisamente la de crear un instrumento de comunicaciones que permitiera evitar la posibilidad de control de las mismas por parte del enemigo militar y político[64]. Como vemos, se trata de un supuesto en el que el objetivo perseguido inicialmente, en un ámbito concreto, presenta inconvenientes posteriormente cuando su uso responde a finalidades que trascienden a las primigenias. De cualquier forma, es obvio que las soluciones localistas en nada resuelven los problemas derivados de un instrumento de naturaleza universal[65].

---

[62] En este sentido, DE ASIS ROIG, AGUSTÍN E. *Protección de datos y derecho de las telecomunicaciones*. En *Régimen jurídico de Internet*. Colección derecho de las telecomunicaciones (coordinadores: Javier Cremades, Miguel Angel Fernández-Ordóñez y Rafael Illescas). Ed. La Ley. MADRID, 2002. Pág. 202.

[63] 5035/01/ES/Final. WP 56. *www.europa.eu.int*.

[64] El origen de Internet se encuentra en ARPANET, una red de comunicaciones del Ejército de EEUU. Consistía en la conexión de un gran número de equipos entre todos ellos, lo cual permitía que, en caso de ataque a uno o varios, la información seguía conservándose. Era necesario destruir todos los componentes del sistema.

[65] De ahí, la necesidad de adoptar instrumentos normativos globales y la conveniencia de las distintas iniciativas de los organismos supranacionales. Por ejemplo, las negociaciones entre la

Por otra parte, el problema de la extraterritorialidad de Internet está conectado con otra cuestión que suscita hoy grandes controversias: la globalización. Nadie puede discutir que la aparición de Internet ha sido decisiva en el desarrollo de este fenómeno, positivo para algunos y negativo para otros. No obstante, la gran mayoría de analistas económicos están de acuerdo en que es necesario frenar algunos efectos que la globalización, junto con un capitalismo de corte salvaje, están generando. A este respecto, se repite con insistencia la solicitud a los Estados para la creación de una regulación de alcance mundial de los mercados financieros, pues la actuación en los mismos a través de Internet ha provocado que los movimientos de capitales sean bruscos, desmedidos e irracionales, provocando grandes convulsiones que, por su carácter global, amenazan la estabilidad financiera mundial[66]. A la misma conclusión se llega si se analiza el nuevo panorama que presenta el crimen o las organizaciones criminales. En definitiva, pretendemos poner de manifiesto que Internet ha supuesto una alteración en la visión regional o nacional de un gran número de cuestiones jurídicas y, por tanto, en su solución.

La extraterritorialidad genera, en principio, mayores problemas derivados de las diferencias de regulación existentes. Como pode de manifiesto De Miguel Asensio[67], si bien EEUU ha optado por la autorregulación, al desechar la elaboración de una normativa sobre Internet, Europa se ha inclinado por la solución contrario. Así, el tratamiento de los problemas jurídicos ocasiona disfunciones y requiere, dada la dispersión mencionada, la adopción de soluciones conjuntas. No estamos, en cambio, de acuerdo con el De Miguel Asensio en que la postura de los EEUU ocasione mayores problemas de protección de los datos de los usuarios de la red. Se trata de una solución que, siendo más acorde con la óptica jurídica anglosajona, puede ser a la vez más eficaz en el objetivo planteado, por cuanto crea soluciones más adecuadas a la práctica.

No obstante todo lo anterior, no debemos caer en la tentación de la novedad y la innovación. No se puede negar que existen cuestiones sobre protección de datos cuya naturaleza y calificación es idéntica, o al menos muy parecida, en el sector de las telecomunicaciones e Internet. Los datos de tráfico y facturación que se generan en ambos no revisten diferencias apreciables que recomienden una regulación

---

UE y EEUU sobre el "puerto seguro". Sobre esta cuestión, MUÑOZ MACHADO, SANTIAGO. *La regulación de la red. Poder y Derecho en Internet*. Ed. Taurus. MADRID, 2000. Pág, 175.

[66] Por citar algunos, GEORGE SOROS. *La crisis del Capitalismo global. La Sociedad abierta en peligro*. Ed. Debate. 1999, MADRID. Pág. 262. También ANTHONY GIDDENS Y WILL HUTTON, eds. *En el límite. La vida en el Capitalismo global*. Tusquets Editores, S.A. 2001, BARCELONA. Págs. 27 y ss., 127 y ss.

[67] MIGUEL ASENSIO, PEDRO A. DE. *Derecho privado de Internet*. Ed. Civitas. MADRID, 2000. Pág. 474.

diversa. Lo mismo podríamos afirmar de otras cuestiones, como las interconexiones o las guías de abonados, entre otros. De lo anterior se deduce claramente que Internet es un sector o tipo entre las diferentes formas de telecomunicación, de lo cual se deduce que la regulación sobre éstas últimas resulta aplicable a la red. No obstante, la fisonomía particular de Internet exige un esfuerzo regulatorio complementario que contemple determinados aspectos que sólo en dicha red se observan. Como se podrá comprobar, la navegación por Internet genera una serie de datos exclusivos, que no se observan en otras formas de comunicación[68]. De esta forma, se puede afirmar, como así ha manifestado el Grupo de Trabajo sobre protección de datos personales, que Internet no es una caso de vacío jurídico[69]. Por el contrario, muchos de los problemas que plantea se pueden y deben resolver a la luz de la normativa de protección de datos existente, tanto la general como la sectorial sobre telecomunicaciones. No obstante, como afirma el citado Grupo, es aconsejable una labor de adaptación de dicha regulación a las particularidades de Internet, así como también resulta necesaria la elaboración de otra específica que acoja las novedades de la misma.

En fin, las particularidades del medio requieren un planteamiento separado y específico de los problemas relativos a la protección de datos de carácter personal, a la vez que debemos replantear problemas existentes en las telecomunicaciones a la luz de la idiosincrasia propia de Internet. Por lo demás, la especificidad no se deduce de la naturaleza de los datos, lo cual se solventaría mediante la aplicación de la normativa sobre protección que cada uno requiera, sino de la naturaleza del vehículo de transmisión. En este sentido, se podría afirmar, salvando las distancias, que *el medio es el mensaje*. No obstante la licencia, ésta no pasa de ser meramente formal, pues como vamos a ver, la normativa existente distingue la regulación de los medios y la de los contenidos, aunque sólo sea en el ámbito de la protección de datos.

Internet plantea, por sus características especiales y su novedad, diferentes problemas en relación con la protección de datos. Sin embargo, debemos puntualizar que, en gran medida, dichos problemas están referidos a la fase inicial de la recogida de datos[70]. No obstante, existen algunas cuestiones que suponen casos de

---

[68] En realidad, no se trata de una tipología diferente de datos. Desde el punto de vista objetivo, aquéllos no presentan diferencias respecto de los generados en otros ámbitos: tráfico, gustos o preferencias, etc. Más bien, se trata de procesos de generación de datos nuevos, los cuales están cualificados por su volumen y la posible información que proporcionan, no por su naturaleza.

[69] GRUPO DE TRABAJO SOBRE PROTECCION DE PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Documento de trabajo: tratamiento de datos personales en Internet (23 de Febrero de 1999).* 5013/99/ES/final. También se encuentra en la página *http://www.europa.eu.int/* (WP 16).

[70] Sostiene Corripio Gil-Delgado que, respecto de Internet, las garantías de la protección de datos deben fortalecer, sobre todo, la fase de la recogida de datos, pues éstos quedan en dicho momento fuera del control del afectado, incluso fuera del país de origen. Se debe observar que tales afirmaciones ponen de manifiesto que la recogida de datos por la red presenta similares

tratamiento y de cesión. Vamos, por tanto, a ceñirnos al análisis de las diversas incidencias que Internet produce en la teoría jurídica de la cesión de datos de carácter personal: datos de tráfico, naturaleza de las cookies, hipervínculos invisibles de terceros en el acto de comunicación, entre otros (respecto de la cuestión relativa a los directorios o guías electrónicas, nos remitimos a lo ya señalado en el apartado anterior). También analizaremos las especialidades que en esta materia presentan el correo y el comercio electrónicos.

2. El ámbito de aplicación de la normativa sobre protección de datos en el sector de las telecomunicaciones e Internet.

Ahora bien, en el ámbito de la protección de datos no todo acto de tratamiento de los mismos se ve sometido a la normativa específica sobre esta materia en el sector de las telecomunicaciones, por el mero hecho de que aquellos actos guarden relación con dicho sector, por razón de los sujetos que intervienen o la forma de realizarla. Las normativas comunitaria e interna establecen un ámbito objetivo estricto por razón del sector, de manera que se evite la superposición de regulaciones, especial y general. Así, la primera se remite a la resolución de problemas relacionados de manera estricta con el medio a través del cual se pueden vulnerar los derechos de los afectados.

El objeto de la Directiva 95/46/CE es la protección de los datos de carácter personal en todo acto de tratamiento, con independencia de los medios que utilicen para llevar a cabo éste. Establece el artículo 3.1 lo siguiente:

> *1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.*

En este sentido, esta normativa se aplica como legislación principal en aquellos supuestos en los que las operaciones no estén sometidas a una regulación especial, así como a todos aquellos casos la misma no establezca una solución para el caso concreto; a la vez que sienta los principios generales sobre la materia en todo caso. Es decir, esta Directiva juega un doble papel: normativa principal en unos casos y subsidiaria en otros. Las mismas afirmaciones se pueden respecto de la LOPD, en el ámbito interno. El artículo 2 de la Ley establece lo siguiente:

> *1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de*

---

características que las cesiones o comunicaciones de datos, aunque obviamente no sean idénticos: alejamiento del afectado de la disposición o control sobre sus datos. CORRIPIO GIL-DELGADO, MARIA DE LOS REYES. *La protección de los datos personales en Internet.* Boletín del Ministerio de Justicia. Año LV. 15 de Septiembre de 2001. Pág. 2918.

tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Por otra parte, la Directiva 2002/58/CE, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), establece un ámbito específico de aplicación, según se deduce de su artículo 3, a saber:

1. La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios públicos de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones en la Comunidad.

Similares exigencias se contemplan, como no podía ser otra manera, en la Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones. El artículo 34, ya mencionado en el Capítulo anterior, establece que

Sin perjuicio de lo previsto en el apartado 6 del artículo 4 y en el segundo párrafo del artículo anterior, así como en la restante normativa específica aplicable, los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público o deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal, conforme a la legislación vigente.

Los operadores a los que se refiere el párrafo anterior deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta ley en esta materia[71]*. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.*

Se puede deducir, sin mayores problemas, que, tanto la Directiva 2002/58 como su antecesora la Directiva 97/66, así como la Ley General de Telecomunicaciones, son ambas de aplicación a las cuestiones sobre protección de datos en Internet. En primer lugar, es indudable que Internet supone la prestación de un servicio público de telecomunicaciones. Unicamente quedarían fuera del ámbito de aquélla los supuestos de tratamiento de datos a través de redes no públicas de comunicaciones electrónicas (en tales casos, se tiene acceso a Internet sin necesidad de mediación de un proveedor de servicios de Internet, sino que la red privada la

[71] Sobre medidas de seguridad de los ficheros que contienen datos de carácter personal, *vid.* Real Decreto 994/1999, de 11 de Junio.

conectan por sí mismos a ésta)[72]. Es decir, la Directiva 2002/58 no es de aplicación a aquellos actos de tratamiento que se llevan a cabo en el seno de una red no pública, por ejemplo, la red interna de una empresa a la que no se tiene acceso público o general. No obstante, tal circunstancia no implica vacío jurídico alguno, pues, como se ha visto anteriormente, tales supuestos se someten a la regulación general.

El carácter público de la red de comunicación utilizada no es el único factor que determina de modo definitivo la aplicación de la Directiva sectorial. Por el contrario, es necesario analizar más detenidamente la expresión *tratamiento de datos de carácter personal en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad*, pues de la misma se deduce otro criterio. ¿Qué implica que el tratamiento deba realizarse en relación con la prestación de los citados servicios?¿Qué circunstancias deben concurrir para que se puedan subsumir tales tratamientos[73] en esta normativa?. En un mismo proceso de navegación en Internet, los usuarios *depositan* información de carácter personal en multitud de ocasiones, ya sea voluntaria o involuntariamente, como vamos a ver. Sin embargo, no todos estos supuestos y los tratamientos que conllevan encajan en el ámbito de la normativa sectorial. La expresión *en relación con la prestación de servicios comunicaciones electrónicas disponibles al público* supone que se regulan por aquélla los tratamientos de datos que sean consecuencia de la prestación de un servicio de comunicación electrónica. Según el artículo 2 c) de la Directiva 2002/21/CE, del Parlamento europeo y del Consejo, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco)[74],

> *c) servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos;…*

En este sentido, sólo los tratamientos de datos que traigan causa de la transmisión y el envío de señales a través de las redes, se consideran dentro del ámbito de aplicación de la Directiva. Así, hay supuestos de tratamiento de datos que no han sido recogidos por los operadores como consecuencia de la prestación del servicio,

---

[72] Tal exclusión se afirma, además, expresamente en el Considerando 11 de la Directiva 97/66/CE.

[73] El término tratamiento debe entenderse en su sentido amplio, de manera que se incluyen en el mismo las diferentes fases u operaciones que se pueden realizar respecto de los datos: recogida, tratamiento en sí y cesión.

[74] DOCE de 24 de Abril de 2002. L 108/39.

sino por razones ajenas al mismo. En estos casos, tales operaciones de tratamiento no revisten especialidad alguna por razón del medio empleado, por lo que se rigen por la normativa general. Solamente se justifica la aplicación de la regulación sectorial cuando el empleo de las redes y la prestación de servicios a través de las mismas han sido elementos determinantes en la captación y tratamiento de los datos. La conexión que un operador de redes facilita a un usuario, con el consiguiente tratamiento de datos de conexión, encaja en el ámbito descrito o la comunicación de datos a través de un formulario que se ofrece en la red. En definitiva, la regulación que estamos analizando se centra en la protección de los datos por razón del acto de comunicación en sí mismo considerado.

Todo lo anterior se observa con mayor claridad si se analiza cada uno de los distintos sujetos que participan en los diferentes pasos de un acto de navegación para facilitar la comunicación por Internet. Cuando un usuario se conecta a Internet con el fin de comunicar con una página, entra en contacto con agentes que cumplen finalidades varias. De modo resumido, podemos citar los siguientes:

a.- *Operador de telecomunicaciones*: es el agente que nos conecta a través de la línea telefónica con el proveedor de acceso a Internet, es decir, el operador tradicional. No obstante, hoy día tales operadores acogen diferentes y novedosas tecnologías de comunicación, que posibilitan la navegación por Internet más allá de la simple telefonía vocal por hilo de cobre: fibra óptica, WAP , UMTS, entre otras[75].

[75] Los términos mencionados hacen alusión, tanto a los cables o vehículos físicos de comunicación como a los sistemas de transmisión. Respecto de los primeros, se pueden distinguir tres tipos: el par de cobre trenzado, el cable coaxial y la fibra óptica. El primero se utiliza para unir el terminal de los abonados con la centralita de la zona en que residan (este recorrido es lo que se conoce como bucle de abonado). Se trata de un medio muy limitado para las posibilidades que ofrecen hoy las comunicaciones, pues su ancho de banda es muy pequeño: no admite, por ejemplo, la transmisión de la señal de televisión. En segundo, el cable coaxial es el empleado para unir los equipos receptores con las antenas de televisión, con una capacidad de transmisión superior al cobre. Finalmente, la fibra óptica se emplea para conectar la centralita con la cabecera (la central). Su capacidad de transmisión es muy superior al resto de los medios citados. No obstante, hoy día existen otros medios de transmisión. Es destacable la transmisión por el espacio radioeléctrico, mediante el empleo de teléfonos móviles, la cual se perfila, a juicio de los analistas sobre telecomunicaciones, como el medio de uso de Internet que finalmente prevalecerá (de hecho, en Japón, país que no se caracterizaba hasta ahora por la utilización masiva de Internet, ha experimentado un incremento en su utilización gracias a la implantación de la tecnología UMTS).
En relación con las conexiones radioeléctricas, ya se han comenzado a desarrollar e implantar algunas tecnologías. En concreto, ya se puede acceder a Internet desde un teléfono móvil por medio del sistema WAP (Wirelles Aplication Protocol, Protocolo de aplicación inalámbrica). Es un protocolo diseñado por un conjunto de empresas fabricantes de teléfonos móviles, que permite acceder a servicios de Internet desde un teléfono móvil que cumple unas especificaciones. No obstante, se trata de un sistema que permite la conexión de modo limitado, dado que el ancho de banda de las licencias actuales es muy limitado para estos usos. El salto a un uso completo viene dado por el sistema UMTS (Universal Movile Telecomunications System). Este sistema permite el acceso a todos los posibles servicios y

a.- *Proveedor de acceso a Internet*: presta el servicio básico de telecomunicaciones, es decir, ofrece las vías (línea telefónica, cable, señal de radio, satélite) a través de las cuales el usuario contacta con el proveedor de servicios de Internet.

b.- *Proveedor de servicios de Internet (P.S.I.)*: se trata de aquel sujeto que nos permite la entrada a Internet de modo general, mediante una conexión TCP/IP. Tal función conlleva otras derivadas de la anterior, como la conexión a páginas concretas, transmisión de contestaciones desde los sitios a los usuarios, etc. En realidad, es quien nos abre las puertas de la red. Hasta este momento, el operador anteriormente citado nos permitía que, en la mayoría de los casos, mediante una llamada telefónica conectáramos con estos P.S.I.

c.- *Página o sitio web*: es el destino de nuestra comunicación, es *el otro lado de la llamada*. Físicamente es un ordenador situado en algún punto de la red, en el que se almacena una determinada información que el usuario desea conocer[76].

Según sea la función desarrollada por aquéllos, se verán sometidos a la regulación sobre protección de datos en el sector de las telecomunicaciones o al régimen jurídico de la legislación general. Los dos primeros agentes citados actúan como transmisores de señales, por lo que sus actos sí encajan en el ámbito de la regulación sectorial, dado que dichas transmisiones generan datos de tráfico, permiten el conocimiento de lo comunicado, así como del equipo desde el que se conecta, entre otros datos. No ocurre lo mismo con las páginas o sitios, pues en estos casos, sólo adoptan la decisión de la información que se pone a disposición de los usuarios en la red, pero no realizan actividad alguna de transmisión o encaminamiento de señales (como sí hacen los routers) en las redes, según determinaba la Directiva 97/66, como ya se ha visto. Estos sitios ofrecen bienes o servicios en general, pero no de

---

goza de grana capacidad de transmisión, incluso de contenidos multimedia (audio, vídeo, datos). Se estima un velocidad de transmisión que podrá alcanzar los 2 M. No obstante, también generará mayores problemas respecto de la protección de datos, pues permite un eficaz tratamiento de las llamadas, control del los servicios prestados y una determinación o localización de la ubicación del usuario.

[76] Podríamos citar otros intervinientes en el acto de navegación: *routers* o encaminadores, portales, prestadores de servicios adicionales y demás. Sin embargo, hemos simplificado tal mención con el fin de clarificar el esquema de la comunicación en Internet.
También debemos señalar que la mención separada de estos agentes no implica que las funciones que desempeñan se presten de forma exclusiva por sujetos diferentes. Por el contrario, en la mayoría de los casos se trata de funciones que se prestan, casi todas ellas, por un mismo sujeto, concretamente por un operador de telecomunicaciones. Así, es normal que tales operadores sean, a la vez, PSI, portales, titulares de páginas, etc. Las anteriores circunstancias traen como consecuencia que tales agentes se verán sometidos a la legislación general y a la sectorial, según sea la actividad que desarrollen en cada momento.

comunicación electrónica. La misma solución se predica de un portal: tan sólo actúa como proveedor de contenidos, no de los citados servicios.

La determinación del régimen jurídico aplicable en los diversos supuestos planteados podría clarificarse en mayor medida con la aparición de la nueva Directiva comunitaria sobre privacidad y comunicaciones electrónicas. La primera diferencia que se observa entre la Directiva 97/66 y la 2002/58 es el cambio que se ha producido en la terminología utilizada para definir el objeto que se regula. En efecto, la segunda Directiva no alude a las telecomunicaciones, sino que se refiere a las comunicaciones electrónicas. La adopción de la nueva terminología pretende, en primer lugar, una adaptación a la empleada por la Directiva 2002/21/CE, que establece una marco regulador común sobre redes y servicios de comunicaciones electrónicas, según se afirma en el artículo 2.1 de aquélla. Lo cual no satisface únicamente un criterio de corrección conceptual y sistémica, sino que además pretende ampliar el ámbito de la norma. En efecto, la definición de servicio de comunicaciones electrónicas, contenida en la Directiva sobre el marco común de bienes y servicios, parece acoger un mayor número de supuestos, según se deduce de su redacción, recogida en páginas anteriores.

Esta definición se extiende más allá de lo que la Directiva 97/66 entendía por servicio de telecomunicación. De hecho, acoge precisamente como uno de los tipos de servicio de comunicación electrónica, los servicios de telecomunicación. La ampliación permite, como vamos a ver a continuación, la inclusión de servicios y medios técnicos que, sin estar incluidos dentro de la legislación sobre telecomunicaciones ni sobre protección de datos en este sector, sin embargo afectaban al régimen de protección de aquéllos. La sofisticación alcanzada permite que las comunicaciones se puedan efectuar a través de redes más amplias que las tradicionales, lo que exige aumentar el régimen de protección de datos.

La primera diferencia que encontramos entre ambas definiciones es la sustitución del término envío por encaminamiento. En realidad, parece que el término transmisión, entendido en sentido amplio, podía englobar aquél. La actividad de encaminamiento, aunque se realiza a la vez que la transmisión y para agilizar ésta, no supone transporte de señal alguno. Como dijimos anteriormente, tal función se desarrolla por los denominados *routers* o encaminadores. Un router es un medio técnico que facilita rutas o caminos de transmisión. Su utilidad está fuera de toda duda, si tenemos en cuenta que las redes soportan grandes cantidades de transmisiones, lo que provoca que sea relativamente normal la sobrecarga y los fallos de conexión, sin olvidar la lentitud de navegación[77]. Como se puede ver, está plenamente justificada la inclusión expresa de dichas actividades, dado el vacío de la normativa en vigor y el tratamiento de datos de carácter personal que aquéllos conllevan.

---

[77] También puede satisfacer otros fines de seguridad, como por ejemplo, servir de cortafuegos entre la red interna de una empresa e Internet.

Como dijimos anteriormente, se incluye en la definición, que por lo demás supera el intento de una concepción general al recoger además una serie de supuestos concretos de servicios de comunicación, los servicios de telecomunicación y las redes de servicios de radiodifusión. Hasta ahora, el sector de la radiodifusión quedaba fuera de la regulación sobre telecomunicaciones, como se deduce indirectamente del artículo 2 d) de la Directiva 97/66. Unicamente se exceptuaban los supuestos de la televisión interactiva y el vídeo por pedido, que sí quedaban recogidos dentro del ámbito de dicha Directiva[78]. Tal excepción ya ponía entonces de manifiesto el profundo cambio que se estaba produciendo. Hoy día no es posible realizar un análisis separado de los servicios de telecomunicación y los medios de comunicación, pues el desarrollo tecnológico ha generado un proceso de convergencia de ambos sectores[79]. Tal circunstancia obliga a que cuestiones como la protección de datos, que

[78] Considerando 10 de la Directiva 97/66/CE.

[79] En el seno de Unión Europea, tal cuestión ha sido objeto de preocupación. Concretamente, la Comisión europea publicó el 3 de Diciembre de 1997 *el libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación (COM (97) Versión 3)*. El libro pone de manifiesto que la citada convergencia de los distintos sectores enunciados se debe producir en tres niveles: el tecnológico, el industrial y el de servicios y mercados, es decir, el de contenidos. La convergencia tecnológica es hoy un hecho, dada la generalización del uso de la tecnología digital. Esta facilita la mejor adaptación de los contenidos a diferentes soportes y su fácil y rápida transmisión a través de distintas redes: piénsese, por ejemplo, en técnicas de compresión MP3 (audio), MPEG (vídeo); la mayor capacidad de transmisión que la señal digital consigue (lo que ha permitido que las televisiones digitales ofrezcan múltiples y simultáneos contenidos, como el pago por visión, la televisión a la carta, canales temáticos, etc.). Igualmente, las tecnologías de red e Internet facilitan el proceso convergente: la primera incide, junto con la digitalización citada, en el aumento de la capacidad de transmisión, dada la aparición de nuevos vehículos (por ejemplo, la fibra óptica); la segunda permite un mayor desarrollo de las actividades de transmisión y oferta de contenidos por su carácter abierto.
En el plano industrial, resulta obvio que se está produciendo, desde hace varios años, un proceso de concentración empresarial que tiene por protagonistas compañías de telecomunicaciones, medios de comunicación y productoras de contenidos. En España, a modo de ejemplo, podemos citar las operaciones que Telefónica ha realizado: adquisición de participaciones en Antena 3, creación de la plataforma Vía digital, compra de la productora de contenidos Endemol. En el caso planteado, la empresa adquirente ha realizado una concentración vertical, al integrar entidades participantes en segmentos no comprendidos inicialmente en la adquirente. Esta circunstancia ha podido plantear, en algunos casos, problemas de competencia.
Finalmente, la convergencia de contenidos es, quizás, la fase que más ha tardado en producirse. No obstante, hoy día es una realidad que hay medios de comunicación, concretamente televisiones digitales, que ofrecen simultáneamente servicios de Internet. La flexibilidad de estas televisiones permite ofrecer descarga de programas de ordenador, juegos, etc. En el mismo sentido incide la radio digital, que admite la combinación de audio y vídeo, entre otros servicios.
Todo lo anterior ha provocado que la Comisión Europea se plantee la conveniencia del establecimiento de una única regulación que acoja realidades cada vez menos diferenciadas, ante la necesidad de eludir los diversos problemas que para el sector en Europa, frente a las

en épocas recientes eran materia exclusiva de la regulación sobre telecomunicaciones frente a los medios de comunicación, también afecten hoy a éstos últimos[80].

Así, la definición de servicios de comunicaciones electrónicas incluye los servicios prestados a través de redes de radiodifusión. No obstante, dicha expresión debe entenderse en su sentido estricto. Al igual que se deducía de la Directiva 97/66, la Directiva sólo establece una regulación relativa a los servicios que consisten en la transmisión y encaminamiento a través, en este caso, de redes de radiodifusión, mientras que los contenidos no son materia de la misma. Así se afirma expresamente en la Directiva 2002/21/CE, cuyo Considerando 5º establece que es necesario separar la regulación de la transmisión de aquella que se ocupa de los contenidos transmitidos[81]. En el ámbito de la protección de datos de carácter personal, tal conclusión resulta de gran importancia, en cuanto determina el régimen jurídico aplicable. Así, todos aquellos supuestos de tratamiento de datos por razón de los contenidos ofrecidos, no del proceso de comunicación, se someten a la regulación general de protección de datos (Directiva 95/46/CE y LOPD, en el caso español). Por lo tanto, las operaciones de tratamiento de datos por parte de proveedores de contenidos o de servicios adicionales, no entran dentro del ámbito de esta Directiva.

Sin embargo, la idea que se deduce de esta solución normativa no es compartida de forma unánime. En el libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación, se pone de manifiesto que existen diversas opciones respecto del carácter único o no de la reglamentación. Quienes

---

empresas provenientes de otras áreas económicas en el mundo, pudiere ocasionar la existencia de una reglamentación fragmentada. Dentro el panorama regulador, también la legislación sobre protección de datos se hace eco de este fenómeno de la convergencia, como ya se ha dicho.

[80] En cualquier caso, las soluciones adoptadas por el legislador continúan con la separación de los regímenes jurídicos de ambos servicios, como se deduce, por ejemplo, de la Ley 32/2002, de 11 de Julio, de servicios de la Sociedad de la información y del comercio electrónico, en cuyo Anexo se establece que no constituyen servicios de la sociedad de la información, entre otros,

- los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3 a) de la Ley 25/1994, de 12 de Julio, por la que se incorpora al Ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de Octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de las actividades de radiodifusión televisiva, o cualquier otra que la sustituya,

- los servicios de radiodifusión sonora, y

- el teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

[81] *Propuesta de Directiva del Parlamento europeo y del Consejo relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.* 12 de Julio de 2000. COM (2000) 385 final.

apoyan la solución unitaria esgrimen razones de naturaleza económica: la necesidad de eliminar obstáculos derivados de la incertidumbre que provoca la variedad normativa, como la existencia de diversos órganos reguladores, regímenes de licencias y demás. También sostiene que la base tecnológica única exige un régimen igualmente único, siquiera manteniendo ciertas especialidades que exijan la diferente naturaleza de los servicios prestados.

Quizás la unicidad normativa responda mejor a las exigencias que impone la convergencia de sectores. Ahora bien, tal necesidad se predica de la adopción de un esquema regulador de las actividades generales de los operadores, pero no parece que exista aquella necesidad en materia de protección de datos. Esta normativa contiene un régimen general, a la vez que acoge especialidades en razón de diversos criterios (tipología de los datos, medios de tratamiento, etc.). Los problemas derivados del tratamiento de datos en el sector de las telecomunicaciones son específicos del medio que los genera, sin que se observen en otros sectores de la actividad humana. Por lo tanto, parece lógico que deba existir esta disgregación normativa. La alegada incertidumbre se torna, en este caso, claridad, de forma que los principios contenidos en la normativa general se aplicarán a todo aquél que lleve a cabo operaciones de tratamiento, sin que los preceptos sobre tratamientos realizados como consecuencia de operaciones de comunicación (datos de tráfico, por ejemplo), puedan aplicarse a quien no desarrolla tal actividad y, por tanto, no se vea inmerso en dichos supuestos. La mayor simplicidad normativa resulta muchas veces, por la naturaleza de las cosas, inviable, cuando dicha reclamación no supone, en realidad, una demanda involuntaria de mayor incertidumbre.

Por otra parte, la Directiva 2002/58, según su artículo 3.1, tan sólo se ocupa del

> *…tratamiento de los datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad.*

En el mismo sentido, el Considerando 10 de la Directiva manifiesta lo siguiente:

> *En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y libertades fundamentales que no estén cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público.*

Finalmente, la definición de los servicios de comunicaciones electrónicas como servicios remunerados, no comporta ningún problema en la determinación del

ámbito de aplicación. Como ha señalado en varias ocasiones el Tribunal de Justicia de la Unión Europea, dicha remuneración puede provenir, no del usuario del servicio, sino de otros sujetos, como los solicitantes de servicios publicitarios. Resulta obvio que tanto la mayoría de los proveedores de acceso a Internet como los titulares de páginas, no reclaman el pago de cantidad alguna a los usuarios. Sin embargo, sí obtienen ingresos de la inclusión de publicidad en las páginas[82]. Además, aunque los usuarios solamente abonan el uso de la línea al operador de telecomunicaciones, sin embargo los proveedores de acceso y los de servicios de Internet obtienen de tales operadores una remuneración (prima de retroconexión) proporcional a la duración de la llamada lo que abunda aún más en el carácter remunerado del servicio.

3. La navegación por Internet y los datos de carácter personal.

La navegación es el proceso en virtud del cual el usuario, mediante la utilización de las líneas ofrecidas por los operadores y mediante el acceso concedido por un proveedor, se conecta con un sitio (o página) concreto ubicado en la red para conocer su contenido e interactuar con aquél, en su caso. Se trata de la modalidad de uso de la red más común. Como hemos observado anteriormente, en el acto de navegación participan diferentes sujetos, que ofrecen diversos servicios. Básicamente, el esquema es el siguiente: mediante una llamada telefónica al proveedor de acceso, éste recibe la información relativa a la página a la que se desea acceder (ya veremos cual es esa información) y asigna un número IP al equipo desde el que se hace la conexión. Tal número acompaña a toda la información que se transmite. La información viaja dividida en paquetes (conmutación de paquetes), los cuales pueden transferirse de forma separada, uniéndose en su destino por el número IP (en realidad, se recogen los números IP del remitente y destinatario), que los identifica y capta el proveedor de acceso.

Una vez que el proveedor ha recibido aquélla, conecta con el sitio solicitado. Hemos de tener en cuenta que, en la mayoría de los casos la navegación, se lleva a cabo mediante el uso de *hipervínculos*. Se trata de un dispositivo que ha facilitado de manera decisiva la navegación por red. Mediante un hipervínculo, el usuario puede navegar desde una página en la que se encuentre a otra, sin necesidad de volver al punto de inicio ni de introducir la dirección determinada, a través de un click del ratón. De forma paralela al beneficio mencionado, los hipervínculos también

---

[82] En realidad, se trata de los ingresos que inicialmente se habían estimado en cantidades superiores a las que realmente se han percibido. De ahí, las grandes pérdidas sufridas por el sector y la crisis bursátil de las acciones de las empresas llamadas *.com*, a finales de los años 90 y principios del siglo XXI. Quizás por esta razón, actualmente existe una gran cantidad de estas empresas que se están planteando el cobro del servicio de acceso.
Sobre esta cuestión, *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea (Documento de trabajo del Grupo de trabajo sobre protección de datos del artículo 29). 5063/00/ES/FINAL (WP 37).* 21 de Noviembre de 2000. También en http://www.europa.eu.int/. Pág. 19.

ocasionan mayores inconvenientes respecto de la protección de los datos de carácter personal, dadas las amplias posibilidades que proporcionan en la navegación[83].

Uno de los elementos más importantes es el uso de los protocolos. Un protocolo es un lenguaje que permite que los equipos que se conectan en la red se puedan entender. Para posibilitar de modo efectivo la navegación, todos los ordenadores conectados a la red *deben hablar el mismo idioma*. El protocolo que permite la conexión, sin más, de los equipos (servidor es el equipo oferente y cliente quien solicita los servicios del anterior) es el protocolo TCP/IP (*transfer control protocol/internet protocol*). Por esta razón, las redes de ordenadores conectados son denominadas redes TCP/IP, las cuales permiten enlazar a las diferentes partes sin necesidad de que exista previa conexión entre ellas, como ocurre en la comunicación telefónica. Ahora bien, este protocolo, por su carácter general, sólo posibilita la transmisión de información en masa. Para la prestación y obtención de determinados servicios se han desarrollado una serie de protocolos específicos: HTTP para la navegación por red, FTP para la transmisión de ficheros; NNTP en el caso de que se desee conectar con un foro; SMTP y POP3, como servidores de correo electrónico saliente y entrante respectivamente.

Pues bien, todas las operaciones mencionadas y la utilización de los medios citados, entre otros, permiten una comunicación rápida y fluida (en la medida de lo posible), que admite una gran variedad de contenidos y posibilidades. De ahí su exitosa irrupción. Sin embargo, también implica la generación de una serie de datos de carácter personal del usuario y su captación por los diferentes sujetos que intervienen, en mayor o menor medida según sus funciones: el operador de telecomunicaciones registra los datos de tráfico, el proveedor de acceso también recoge éstos, a la vez que identifica la llamada que recibe, conoce la dirección IP que él mismo adjudica al equipo del cliente[84], registra los datos de las conexiones concretas efectuadas, guarda los sitios visualizados desde un número IP concreto, etc.; los proveedores de servicios, como los portales, registran las páginas *colgadas* en el mismo que se han visitado, los datos de navegación, envían *cookies* al equipo cliente. Existen otros sujetos que intervienen, los cuales también acceden a información de distinta naturaleza.

---

[83] Por ejemplo, el uso de hipervínculos permite a los usuarios saltar las fronteras nacionales, lo cual dificulta el control sobre los datos y las posibles actuaciones e los órganos de control. AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria 2000*. Pag. 185.

[84] La dirección o número IP que se adjudica al equipo es dinámico, es decir, varía de una conexión a otra, siempre que la conexión se efectúe a través de un modem (por lo tanto, no siempre es así, sino que depende del tipo de conexión. Por ejemplo, en una conexión mediante ADSL o en la telefonía móvil, la dirección asignada es estática, aunque en los últimos tiempos los operadores pretende ofrecer IP´s dinámicas). Aunque tal circunstancia pudiere hacernos pensar que se oculta de esta forma el equipo desde el que nos conectamos, sin embargo el servidor y los sitios saben que en una determinada conexión tal ordenador tenía tal número.

En la mayoría de los casos, se trata de supuestos de recogida o captación de datos, prestados directa y, en gran medida, involuntariamente por el propio usuario. En efecto, los datos de que gozan los distintos intervinientes en el proceso, son ofrecidos por el usuario, que desconoce los diferentes elementos técnicos y sus posibilidades. No obstante, también existen supuestos de cesión o comunicación de datos de carácter personal generados y captados con ocasión de la navegación por Internet. El análisis del tratamiento de los datos se complica si tenemos en cuenta que el carácter transnacional de la red hace que la vigilancia de este tipo de operaciones resulte en ocasiones prácticamente imposible. A lo anterior se debe añadir la vulnerabilidad de las bases de datos alojadas en equipos conectados a la red.

Pues bien, todas las circunstancias anteriores ponen de manifiesto la necesidad que poseen los usuarios de Internet de que se les proporcione, por los responsables de los diferentes ficheros en que se almacena los datos personales, información al respecto. A tal efecto, la Recomendación del Grupo de Trabajo del artículo 29 sobre determinación de los requisitos mínimos para la recogida en línea de los datos personales en la Unión Europea (adoptada el 17 de Mayo de 2001)[85], afirma que al usuario se le debe facilitar previamente la siguiente información: identidad y dirección del responsable del fichero, fines del tratamiento, carácter obligatorio o no de la información solicitada, derechos de consentimiento, oposición, acceso, rectificación y cancelación; destinatarios o cesionarios, en su caso; encargado de contestar a las preguntas sobre protección de datos; y medidas de seguridad. Esta información debe aparecer de forma clara en pantalla. Además, se recuerda que solamente se deben recoger los datos necesarios para satisfacer fines legítimos, los cuales determinan, además, el período de tiempo de almacenamiento.

Antes de iniciar el examen de estas cuestiones, la posibilidad de no determinar, directamente o indirectamente, quien es el cesionario o receptor de los datos, según se deduce del artículo 11 *sensu contrario* (la LORTAD si establecía esta exigencia), posibilita que un mayor número de cesiones o comunicaciones de datos a través de la red resulten lícitas, ante el masivo incumplimiento de este requisito por los distintos operadores de la red[86].

a. Los datos de tráfico en la navegación por Internet.

La naturaleza de los datos de tráfico ya ha sido tratada en el Capítulo anterior, relativo a las comunicaciones telefónicas. Sin embargo, las soluciones apuntadas entonces, si bien sirven como punto de partida y no se alejan excesivamente de las que se proponen a continuación, requieren alguna explicación añadida a las anteriores, dadas las especialidades del medio, como ya hemos dicho. Concretamente, los mayores o menores problemas que pudiéramos encontrar a la hora de calificar los datos sobre tráfico como parte del contenido de una comunicación, se desvanecen en

[85] 5020/01/ES/Final. WP 43. *www.europa.eu.int*.

[86] CASTRO REY, JOSE LUIS. *Op. cit.* Pág. 34.

gran medida cuando la misma se realiza a través de Internet. El modo en que se comunica por este medio implica la imposibilidad de poder distinguir, en la mayoría de los casos, entre información sobre el formato o esquema del acto de comunicación y su contenido. Por lo tanto, desde este momento podemos afirmar que la protección normativa que se debe brindar a los datos sobre tráfico debiera ser la misma que la que recibe el objeto de la comunicación. No debemos olvidar que la solución aportada por la Fiscalía General del Estado en la Circular 1/99, estudiada en líneas anteriores, resolvió las dudas que se planteaban en relación con un supuesto de comunicación entre ordenadores conectados a Internet, en el que se produjo un vaciado inconsentido de datos entre ambos. Ello no implica una solución distinta y específica para las comunicaciones a través de Internet, diferente de las comunicaciones por telefonía tradicional, como sostuvo la Fiscalía. Pretendemos señalar que en la navegación por Internet la confusión entre datos de tráfico y contenido de la comunicación se observa con mayor claridad que en el caso anterior (sin negar que en el mismo existan razones para adoptar idéntica solución, según ya se dijo).

La comunicación por Internet genera mayor número de datos atinentes al tráfico que los que obtiene un operador de telecomunicaciones en una comunicación telefónica tradicional. La característica de la interactividad es un de los factores que provocan tal aumento. Un solo click del ratón genera un flujo de datos (*clickstream data)*, por lo que podemos hacernos una idea de todos los que se generan en una sola conexión a Internet, en la que generalmente el usuario accede a distintos sitios. Debemos tener en cuenta que a los datos sobre la llamada en sí que inicialmente supone la navegación, se unen los datos que la utilización de un programa de navegación produce. Además, gran cantidad de esta información se guarda por los proveedores de acceso en los denominados *archivos log*.

En efecto, el peligro de la interceptación de las comunicaciones realizadas a través de Internet es, por el número de datos generados, mayor, si cabe, que en las comunicaciones telefónicas tradicionales. Sin olvidar que la digitalización de la información y el carácter informático de los medios empleados para acceder a dichas comunicaciones, hace que estas labores resulten más fáciles y con mayores posibilidades de éxito. En este sentido, no está de más abogar por un régimen de control de las interceptaciones más riguroso. Actualmente, el incremento de este espionaje es exponencial y se ve agravado porque el mismo se lleva a cabo, o se pretende realizar, de forma invisible o desconocida para los interlocutores[87]. Hoy día,

---

[87] En este sentido, hemos de señalar que el control de estas actividades resulta difícil, pues las mismas escapan al conocimiento e investigación de los órganos nacionales pertinentes. Lo anterior se agrava por el hecho de que tales sistemas tiene por objetivo la escucha de ciudadanos y entidades que no son nacionales del país espía, por lo que sus órganos parlamentarios, por ejemplo, muestran escaso interés en traspasar el velo que caracteriza a estos servicios de información, dado que sus electores no se ven, en principio, afectados. Sobre estas cuestiones, PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON. *Informe sobre la existencia de un sistema mundial*

uno de los ejemplos que ilustran lo que decimos lo constituye la controvertida red *Echelon*.

A mediados de la década de los 90 se empieza a tener conocimiento[88], no corroborado inicialmente, de que la NSA (National Security Agency o Agencia de Seguridad Nacional, organismo del Gobierno de E.E.U.U. encargado de controlar las telecomunicaciones), en compañía de su homólogo inglés, habían creado una red conjunta que permite interceptar todas las comunicaciones que se producen en el mundo. Para ello, emplean instalaciones ubicadas en sus territorios nacionales, además de Canadá, Australia y Nueva Zelanda, según parece. En 1997 un espía británico hizo unas manifestaciones afirmando la existencia de esta red, lo que motivó el interés del Gobierno holandés, que en aquel entonces ostentaba la Presidencia de Unión. Incluso, ha habido filtraciones procedentes de supuestos trabajadores de Echelon y los servicios de contraespionaje franceses han investigado esta red, por motivos de defensa de compañías francesas con problemas de espionaje industrial.

A pesar de las negativas de las autoridades estadounidenses e inglesas sobre su existencia, lo cierto es que el Parlamento Europeo aprobó la creación, con fecha 5 de Julio de 2000 (se fijó el plazo de un año de duración desde su creación), de una Comisión de investigación que analizase el uso de los satélites por E.E.U.U. y el Reino Unido. Pues bien, la Comisión de investigación concluyó un informe el 11 de Junio de 2001, aunque se presentó a la opinión pública los primeros días de Septiembre. En el mismo se afirma que *ya no cabe ninguna duda en cuanto a la existencia de un sistema de interceptación mundial de las comunicaciones que funciona con la participación de los E.E.U.U., del Reino Unido, del Canadá, de Australia y de Nueva Zelanda, en el marco del acuerdo UKUSA*[89] (UKUSA es el acrónimo de United Kingdom y United States of America, el cual hace referencia a un convenio sobre inteligencia firmado en 1948 por E.E.U.U., Reino Unido, Australia, Canadá y Nueva Zelanda, y en virtud del cual las partes acuerdan intercambiarse información)[90].

---

de interceptación de comunicaciones privadas y electrónicas (sistema de interceptación ECHELON). Ponente: Gerhard Schmidt. 11 de Julio de 2001. FINAL A5-0264/2001 PARTE 1. Págs. 28-29.

[88] Duncan Campbell, periodista británico, tuvo constancia de la red de forma inesperada, al comprobar que los cables de una aparente radiotelescopio terminaban en una base militar.

[89] PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON. *Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y electrónicas (sistema de interceptación ECHELON)*. Ponente: Gerhard Schmid. 11 de Julio de 2001. Págs. 19-20. FINAL A5-0264/2001 PARTE 1. El informe se puede encontrar en el sitio http://www.europarl.eu.int/.

[90] PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON… Págs. 64 y ss.

En el fondo de toda esta polémica se están dirimiendo intereses de naturaleza económica, más que la defensa de derechos individuales. En efecto, la principal preocupación de algunos Estados europeos residía en el hecho de que esta red se estaba utilizando, al parecer, para realizar tareas de espionaje industrial en beneficio de compañías estadounidenses. Concretamente, la información conseguida a través de aquélla permitió, siempre sin confirmar, la pérdida de contratos por parte de empresas como Airbus o Thomson-CSF a favor de otras como McDonnell-Douglas o Boeing[91].

A pesar de la postura beligerante de países como Francia y Alemania frente a estas supuestas actividades, sin embargo parece ser que han proliferado los intentos de los Estados por procurarse un sistema de estas características. Francia aprobó el 28 de Junio del 2000 (curiosamente dos días antes de asumir la Presidencia de la Unión en el momento en que se crea en el Parlamento europeo la Comisión antes citada) la Ley de libertad audiovisual[92], en la que se exige a los proveedores de servicios el almacenamiento de la información sobre los usuarios, sin determinar de forma explícita los posibles fines de esta información. El informe de la Comisión del Parlamento europeo destaca que Francia podría ser uno de los pocos países en el mundo que pudiera desarrollar un sistema de interceptación de cobertura mundial, al disponer de territorios en las tres áreas en las que se requiere instalar los medios

---

[91] La revista alemana *Der Spiegel* informó de que el mismo George W. Bush, informado de las interceptaciones de comunicaciones entre la empresa japonesa NEC y el Gobierno de Indonesia, presionó a éste último para que, finalmente, el contrato que inicialmente se había celebrado con la primera para la realización de un satélite por valor de 200 millones de dólares, se compartiera con ATT. En el mismo sentido, las interceptaciones de conversaciones entre el Gobierno brasileño y la empresa francesa Thomson-CSF provocó que el contrato para la elaboración de un radar (1,3 millones de dólares) se firmara finalmente con la estadounidense Raytheon. Estos y otros casos no son reflejo de una actitud aislada. Por el contrario, las consecuencias económicas derivadas de la posición ventajosa que obtiene el sector económico estadounidense no es desdeñable: un informe del Congreso de los E.E.U.U. estimó que las empresas del país ganarían alrededor de 7000 millones de dólares. PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON… Pág. 18.

[92] Esta ley se puede encontrar en http://www.assemblee-nationale.fr/2/2textes-a.html . Además, tal normativa no resulta acorde, como vamos a ver a continuación con las previsiones que al respecto a realizado el Grupo de Trabajo del artículo 29. Concretamente, se aconseja la adopción, en la medida de lo posible, del anonimato y se rechaza la posibilidad de que los servidores almacenen la información sobre datos de tráfico y navegación por razones de cumplimiento de la legislación. Tales conclusiones son las ideas centrales del GRUPO DE TRABAJO SOBRE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Recomendación 3/99, sobre la conservación de los datos sobre tráfico por los proveedores de servicio de Internet a efectos de cumplimiento de la legislación* (7 de Septiembre de 1999). 5085/99/ES/FINAL. *Recomendación 3/97, sobre Anonimato en Internet* (3 de Diciembre de 1997). XV D/5022/97 ES final.

técnicos necesarios (Europa, América, pues en el Atlántico cuenta con posesiones en el Caribe, y en Asia, pues posee islas en el Océano Indico y en el Pacífico)[93].

Igualmente, el Reino Unido aprobó la Regulation of Investigatory Powers Bill, que establece exigencias excesivas para los servidores y ha sido objeto de repulsa (Colegios de abogados, asociaciones de derechos de los usuarios de Internet, de medios de comunicación, entre otros)[94]. El informe citado señala igualmente que Rusia podría haber desarrollado un sistema idéntico a través de la Agencia Federal de Comunicaciones e Información del Gobierno (FAPSI), puesto que posee estaciones de interceptación, además de en el propio territorio ruso, en Letonia, Cuba, Vietnam del Norte y en algunas islas del Océano Indico. Precisamente por no tener acceso a las distintas áreas geográficas para la instalación de equipos, se descarta tal posibilidad respecto de China u otros países del G-8[95].

Como ya hemos señalado anteriormente, las finalidades del sistema Echelon son, principalmente, de naturaleza económica, lo que implica su utilización en la interceptación de comunicaciones relacionadas con personas privadas o con labores de espionaje industrial, conforme se deduce del título del informe del Parlamento Europeo[96]. En el mismo sentido, en otro pasaje de este informe se afirma que *ya no cabe duda de que la finalidad del sistema es la interceptación, como mínimo, de comunicaciones privadas y económicas, y no militares,…*[97]. La determinación estricta de las

---

[93] PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON… Págs. 83 y ss.

[94] La normativa inglesa se puede consultar en http://www.silicon.com/a38414.

[95] PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON… Págs. 84 y 85.
No obstante lo anterior, Rusia ha anunciado, con posterioridad al citado informe, y a los atentados en E.E.U.U. de Septiembre de 2001, su decisión de desmantelar las estaciones de Lourdes (Cuba) y de Cam Ranh (Vietnam del Norte), con el fin de adquirir material de observación (satélites y radares) más moderno. EL PAIS, 18 de Octubre de 2001.

[96] Señala el Considerando P del informe lo siguiente: *considerando que los servicios de inteligencia de los Estados Unidos no sólo informan sobre la situación económica general sino que además escuchan detalladamente las comunicaciones de las empresas precisamente cuando se trata de la concesión de contratos, justificando tal actividad con la lucha contra la corrupción; que, en el caso de las escuchas detalladas, existe el peligro de que la información no se utilice para luchar contra la corrupción sino para espiar a la competencia, por mucho que los Estados Unidos y el Reino Unido declaren que no lo hacen; que sigue sin estar claro el papel que desempeña el Advocacy Center (Centro de Interlocución) del Departamento de Comercio de los Estados Unidos, y que una reunión que iba a tener lugar para aclarar este asunto fue suspendida.* PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON… Págs. 17 y 18.

[97] PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON… Considerando B. Pág. 15.

finalidades del sistema Echelon tiene una importancia decisiva a la hora de establecer las posibles vulneraciones de los diferentes instrumentos jurídicos que regulan la protección de datos. Según establece el artículo 15.1 de la Directiva 2002/58,

> *Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las derechos y obligaciones que se establecen en los artículos 5 y 6* (sobre confidencialidad de las comunicaciones y datos de tráfico y facturación, respectivamente) *y en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva* (sobre identificación de las líneas llamante y conectada y datos de localización) *cuando tal limitación constituya una medida necesaria proporcionada y apropiada para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, la investigación, la descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46*[98]…

En un sentido similar se pronuncia el artículo 13 de la Directiva 95/46. En primer lugar, tenemos que señalar que, si bien alguno de los miembros de esta red no lo es de la Unión europea, sin embargo no es así en todos los casos, pues entre ellos está el Reino Unido. Por lo tanto, existe la posibilidad de aplicar la Directiva comunitaria a las actividades de tratamiento de datos obtenidos de las interceptaciones realizadas mediante el empleo de este sistema por parte de GCHQ británico (Government Communications Headquarter). Tal circunstancia elimina la posibilidad de excluir la aplicación de la Directiva 2002/58/CE, sobre privacidad de las comunicaciones electrónicas, al caso en cuestión[99].

---

[98] En relación con estos criterios de limitación, el artículo 1.3 de la Directiva 97/66 incluía, dentro del concepto de seguridad del Estado, *el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del Estado*. Tal expresión no puede hacerse extensiva a los intereses económicos de las empresas y corporaciones, por muy decisivos y estratégicos que sean, dado que los mismos no contienen el ingrediente de naturaleza pública que se observa en la mención seguridad del Estado.

[99] El artículo 4.1 c) de la Directiva 95/46 establece que serán de aplicación las disposiciones nacionales de desarrollo de esta Directiva cuando *el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de los datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en el caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.* Este podría ser el caso, por ejemplo, de la estación de interceptación estadounidense de Bad Aibling (Alemania), donde, en principio, sólo existen antenas de recepción de señal de satélite. Ahora bien, aunque la información recogida de esta forma se envíe a otros centros fuera de la Unión Europea para su posterior estudio y análisis, en realidad la concepción amplia del término *tratamiento* acogida en la citada Directiva, el cual incluye la recogida, permite afirmar que, salvo que el tránsito de la señal no permita la permanencia de la información en la estación, tales actividades también se incluyen en el ámbito de aplicación de aquélla. No obstante, como hemos señalado, en la estación británica de Menwith Hill trabajan, no sólo los servicios norteamericanos, sino los propios británicos, lo

Por otra parte, resulta obvio que las finalidades a las que se destinan tales medios no son compatibles con los objetivos que las dos Directivas recogen como presupuestos de exclusión. Las Directivas fundamentan las excepciones señaladas en el mantenimiento de una seguridad común a todos los ciudadanos de un Estado, no en la circunstancia de que la realización de las actividades se lleven a cabo por uno u otro organismo del Estado. En este sentido, como se puede comprobar, la normativa comunitaria ha acertado plenamente al no admitir como presunción incontestable el interés general de los actos de los organismos públicos, dado que las interceptaciones a través de Echelon se realizan sobre sujetos o entidades particulares, para la satisfacción de intereses igualmente particulares: es lo que se conoce como espionaje industrial o de competencia, lo cual excluye las labores de información con fines militares, de seguimiento de grupos terroristas y, en general, cualesquiera otras propias de la actividad exclusiva y lógica de los Estados[100].

Tampoco debemos olvidar que la Directiva 2002/58 no sólo pretende proteger los derechos fundamentales de las personas físicas. El artículo 1.2 establece *la protección de los intereses legítimos de los abonados que sean personas jurídicas*. No cabe duda de que los lícitos objetivos económicos de las empresas europeas están presentes en esta norma.

En definitiva, todos estos argumentos permiten afirmar que la legislación sobre protección de datos resulta de aplicación a los casos de interceptación de comunicaciones mediante el empleo de la red Echelon. No obstante lo anterior, la cobertura normativa es más amplia, puesto que los actos que se analizan inciden de forma directa en el ámbito objetivo del secreto de las comunicaciones, lo que implica la posibilidad de que puedan derivarse responsabilidades tanto civiles como penales.

Otro ejemplo de sistemas de interceptación de comunicaciones en general es el programa Carnivore (Carnívoro). El Carnivore (rebautizado DCS100, quizás con el fin de aminorar la carga peyorativa que conlleva la denominación inicial)

---

que elimina las dudas respecto de la aplicación de la normativa comunitaria. Esta intervención de un Estado miembro resulta contraria al principio de lealtad entre los Estados miembros, que se recoge en el artículo 10 del TCE, el cual obliga a no realizar actos que puedan ir en contra de los objetivos del Tratado, entre los que se encuentra la libre competencia, según se afirma en el informe del Parlamento Europeo.

[100] Tras los ataques terroristas a Nueva York y Washington, las autoridades de E.E.U.U. han reconocido de forma indirecta la existencia de Echelon, a la vez que han manifestado su intención de reforzar estos servicios de información. En tal caso, la normativa sobre protección de datos podría no ser aplicada, en cuanto que los fines de tales actos se encuadran dentro de las excepciones del artículo 1.3 de la Directiva 2002/58 (actividades dirigidas a la seguridad pública, la defensa, la seguridad del Estado y actividades de éste en materia penal). No obstante, tales justificaciones no eliminan la necesidad de que concurran los requisitos que el TEDH exige para la interceptación de las comunicaciones, sobre todo legalidad y proporcionalidad

es una aplicación empleada por el FBI (Federal Bureau of Investment), en virtud de la cual se vigilan, interceptan y analizan grandes volúmenes de mensajes de correo electrónico. Para conseguir tal fin, se instala el programa en los proveedores de servicios de Internet, de forma que se pueden conocer los datos de tráfico y navegación así como los contenidos de los mensajes que envían los usuarios que utilizan dichos servidores y de todos aquéllos que conecten con éstos. Además, discrimina los mensajes que contienen determinados términos que interesan por motivos de investigación criminal (terrorismo, tráfico de drogas, etc.), para lo cual utiliza sistemas de filtro o diccionarios.

Los proveedores conocen tal posibilidad por la instalación del programa, pero no saben cuando se utiliza de forma efectiva. No existe autorización judicial previa, según exige la legislación de los E.E.U.U, pues la misma se requiere, lógicamente, para cada acto de interceptación. Cuando el programa detecta un mensaje que pueda interesar por su contenido, se introduce en el disco duro del equipo de quien navega por Internet y capta la información albergada en el mismo. Las dudas que este sistema planteaba respecto de la protección de la privacidad de los usuarios han aumentado a raíz de las modificaciones legislativas que se han producido en E.E.U.U. después de los atentados del 11 de Septiembre. A propuesta del Fiscal General, se ha adoptado la *Anti-terrorism Act* (ATA, 19-9-2001), en virtud de la cual se otorgan mayores posibilidades de vigilancia de las comunicaciones electrónicas, al eliminar la necesidad de una autorización judicial previa para las interceptaciones. Concretamente, el FBI podría instalar el Carnivore sin necesidad de autorización judicial hasta que transcurran 48 horas[101]. Programas parecidos parecen implantarse en otros países como Japón (el programa se denomina Kari-no-mail, algo así como el buzón temporal) o Noruega (aunque la intención inicial del programa es filtrar los posibles virus y demás contenidos irregulares, sus responsables han manifestado que también está capacitado para interceptar los mensajes de correo electrónico en general).

Quizás, se podría argumentar que, si bien los primeros son verdaderos datos sobre tráfico, no ocurre lo mismo con los segundos, los cuales se encuadran correctamente dentro del ámbito de los datos sobre el contenido de la comunicación. Sin embargo, tales argumentos están lejos de la realidad de la navegación por Internet. Como vamos a ver, los datos sobre navegación se encuadran perfectamente dentro de la definición propuesta de datos sobre tráfico. A la profusión de datos antes señalada, se une la elevada configuración técnica de Internet, que hace que la posibilidad de recogida de datos personales sea mayor ante la mejor calidad de los programas de búsqueda y recopilación. En un acto de navegación se generan los siguientes datos:

---

[101] Parece ser que tales hechos ocurrieron en los instantes inmediatos a los atentados, en los que el FBI apareció en las sedes de los tres mayores proveedores de correo electrónico (AOL, Hot Mail y Earthlink) y comenzó a intervenir las comunicaciones y a examinar las realizadas por determinadas cuentas o con términos concretos.

1.- en primer lugar, los datos de tráfico propios de una llamada telefónica (la que realizamos al proveedor de acceso), que se registran por el operador de telecomunicaciones.

2.- El proveedor de acceso a Internet registra la identificación de la línea desde la que se hace la llamada. Además, se guardan los datos sobre la sesión concreta: nombre de la conexión, hora de la misma y de la desconexión y los datos transferidos. Respecto de estas entidades, la Agencia Española de Protección de Datos, en la Memoria del año 2000, recoge un estudio sobre las prácticas de tres servidores de acceso respecto de la protección de los datos de sus abonados y de los visitantes de las páginas alojadas en sus sitios. Entre otras conclusiones, se afirma que los servidores pueden conocer cual es la identidad de dichos visitantes, siempre que los mismos accedan a la red a través de aquéllas, dado que las mismas son quienes proporcionan a aquéllos la dirección IP. A pesar de que la conservación de tales datos en los registros se justifica por la conveniencia de mantener el servicio, sin embargo dos de las tres entidades no han borrado los datos almacenados desde que comenzaron a prestar el servicio[102].

3.- Los portales, que han proliferado debido a que ordenan los sitios y permiten que el usuario discrimine las opciones sobre éstos, registran las visitas efectuadas a los sitios alojados en aquél, lo que permite elaborar un perfil de los usuarios ante las preferencias que manifiestan en la navegación (esto resulta de máximo interés para los titulares del portal, dado que, generalmente, éstos contienen sitios de carácter comercial), sin olvidar los datos recabados a través del envío de cookies al disco duro del ordenador cliente.

4.- Las páginas o sitios visitados también recaban datos: las visitas realizadas a los mismos, registran las páginas de procedencia y las claves utilizadas (tales datos también se recogen por el proveedor de servicios, generalmente a través de portales). La utilización de programas de navegación (los más conocidos son Internet Explorer y Nestcape Navigator) permite que los sitios tengan conocimiento de mayor cantidad de datos: sistema operativo utilizado, tipo de navegador, protocolos, página de procedencia, idioma, cookies. Tal información, unida a la proveniente del uso de otros dispositivos, se amplía: país, sector de la empresa y su volumen, puesto del usuario, sitios visitados, entre otros.

¿Qué debemos entender por datos de tráfico?. Como ya se ha visto en páginas previas, La Directiva 2002/58 define éstos, en el artículo 2 b) como *cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma.*

El artículo 65.1 del Real Decreto 1736/1998, de 31 de Julio, por el que se aprueba el Reglamento de desarrollo del Titulo III de la Ley General de

---

[102] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 2000*. Pág. 203.

Telecomunicaciones, contiene una redacción similar a la del artículo 6 de la Directiva 97/66, la cual no difiere, a su vez, de la definición contenida en la Directiva de 2002. Atendiendo a la terminología empleada, el concepto de datos sobre tráfico tiene un claro sentido finalista. Así, se trata de información que los operadores necesitan para establecer las comunicaciones solicitadas, así como para facturar correctamente las que se han efectuado. Por lo tanto, tal definición hace referencia a los datos necesarios para poder conectar a las partes de una comunicación y cobrar el servicio prestado, es decir, datos generados como consecuencia de la comunicación en sí, a efectos de la misma.

Conscientes de las limitaciones de la Directiva 97/66, cuyos artífices pensaban más bien en las comunicaciones por telefonía vocal, la Directiva 2002/58 define los datos de tráfico de forma más amplia. Dado que la navegación por Internet genera datos relativos no sólo al tráfico en sí, sino también atinentes al contenido, el artículo 2 c) incluye, no sólo los datos que son necesarios para el establecimiento de la comunicación, los datos tratados a efectos de la misma. Además, reciben dicho tratamiento los datos generados *en el curso de la comunicación* a través de la red. Por lo tanto, también reciben dicha calificación aquellos datos que, siendo necesarios para la navegación, sin embargo no sean estrictamente necesarios para establecer la comunicación.

En relación con lo anterior, el artículo 5 de la Directiva 2002/58 establece lo siguiente:

> *1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos sobre tráfico asociados a ellas, realizadas a través de redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando estén autorizados legalmente a hacerlo, de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad.*
>
> *2. El apartado 1 no se aplicará a las grabaciones legalmente autorizadas de comunicaciones y de los datos sobre tráfico asociados a ellas cuando se lleven a cabo en el marco de una práctica comercial lícita con el fin de aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial*[103].

[103] Pensemos, por ejemplo, en la grabación que las Agencias y Sociedades de valores efectúan de la conversación mantenida entre el operador y el cliente, exigida como medio de prueba por la legislación del mercado de valores.

Aunque el precepto, cuya leyenda reza *confidencialidad de las comunicaciones*, hace alusión en primer lugar, al contenido de las comunicaciones, sin embargo en la navegación por Internet no parece que se pueda establecer una nítida separación entre datos de tráfico y de navegación. Como hemos señalado, diferentes agentes pueden conocer los sitios a los cuales se ha accedido. Pues bien, tal información es, en realidad, información sobre el contenido de la comunicación, dado que la simple visualización de las páginas visitadas, que se conocen mediante los datos de tráfico, permitirá a quienes tengan esta información conocer cuál ha sido el contenido y sentido de aquélla.

Por esta razón, parece lógico que el artículo 5 de la Directiva haga alusión expresa a la confidencialidad de los datos de tráfico asociados a las comunicaciones. Se trata de una novedad importante, pues la Directiva 97/66, en su artículo 5.1, solamente exigía a los Estados miembros la garantía de *la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público*, sin que se mencionen los datos sobre tráfico. En relación con esta cuestión, el Grupo de Trabajo del artículo 29 ha sostenido que los datos sobre navegación deben recibir la misma protección que los contenidos que se deducen de la misma, a lo cual añade que, ante la definición de datos de tráfico antes mencionada, los datos de navegación deben ser considerados datos sobre tráfico[104].

Ahora bien, no estamos de acuerdo con la calificación de los datos de navegación como datos de tráfico, exclusivamente. Efectivamente, algunos de estos datos son necesarios a efectos de la comunicación. No obstante, muchos de estos datos revelan además información de la comunicación. Es decir, parece que tal información tiene una naturaleza híbrida, de manera que no es posible separar ambos aspectos, al menos no respecto de todos los datos de navegación. A tal conclusión llega, a nuestro entender con acierto, el Grupo de Trabajo del artículo 29, al afirmar que

> …*En un primer momento, los datos relativos a ésta* (la navegación) *podrían considerarse datos sobre tráfico. No obstante, el Grupo de Trabajo opina que navegar por distintos sitios podría considerarse una forma de comunicación y, como tal, debería quedar cubierta por el ámbito de aplicación del artículo 5*[105].

Los datos de navegación se configuran como una categoría que impide el desdoblamiento que la regulación tradicional establecía entre contenido y tráfico, entre mensaje y medio. En la navegación por Internet no se generan datos referidos

---

104 *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea (Documento de trabajo del Grupo de trabajo sobre protección de datos del artículo 29)*… Pág. 56.

105 *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea (Documento de trabajo del Grupo de trabajo sobre protección de datos del artículo 29)*… Pág.

estrictamente a ninguno de los aspectos mencionados, sino que se presentan de forma indisoluble ambas informaciones. En realidad, nosotros entendemos que, si los datos de tráfico muestran en cierta medida información del mensaje en el caso de la telefonía vocal, sin embargo en Internet tal afirmación resiste cualquier afirmación en contra. La configuración de los datos de navegación permite sostener que se trata de un tercer tipo. En tal sentido se manifiesta el Grupo de Trabajo del artículo 29, al afirmar:

> *La revisión de esta Directiva* (Directiva 97/66) *ha entrañado otras mejoras gracias a la ampliación del ámbito de aplicación del artículo 5 para abarcar no sólo el contenido de la comunicación, sino también los datos sobre tráfico correspondientes. Al ofrecer la misma protección al contenido que a los datos sobre tráfico relacionados con él se resta importancia a la distinción, no siempre evidente, entre estos conceptos. El Grupo de Trabajo acoge favorablemente esta mejora.*

De las anteriores manifestaciones parece deducirse que los datos sobre tráfico admiten una clasificación doble: por una parte, los datos de navegación, a los que alude el Grupo de Trabajo cuando menciona *los datos sobre tráfico relacionados con él* (el contenido); por otra, los datos de tráfico en sentido estricto. De esta forma, la equiparación con el contenido de la comunicación sólo se predica de los primeros, nunca de los segundos que sólo hacen referencia a los aspectos formales de aquélla. Sin embargo, no estamos de acuerdo con tal posibilidad. Es cierto que el artículo 2º de la Propuesta de Directiva sobre privacidad y comunicaciones electrónicas, afirmaba que son datos de tráfico los tratados *en el curso o a efectos de la transmisión de una comunicación*, con lo que parece distinguir entre datos de navegación y datos de tráfico en sentido estricto, respectivamente. Ahora bien, tras establecer tal distinción, en ningún momento afirma que los datos generados a efectos de la comunicación no hagan referencia al contenido de la comunicación. Quizás por esta razón, el definitivo artículo 2 b) de la Directiva 2002/58 solamente alude a datos tratados *a efectos de la conducción de una comunicación*.

Desde un punto de vista normativo, la Directiva 2002/58 exige, como hemos visto, el mantenimiento de la confidencialidad de los datos sobre tráfico *asociados a las comunicaciones*, sin distinguir con arreglo al criterio de la referencia o no al mensaje. Por lo tanto, los datos sobre tráfico reciben la misma protección que el contenido de las comunicaciones, sin que se matice tal régimen en función de la aparente clasificación del artículo 2. Poca virtualidad tienen las distinciones teóricas si en la práctica la solución normativa aplicable a las diversas situaciones es idéntica. Esta consecuencia ha sido sostenida, aunque no de forma muy decidida, por el Grupo de Trabajo en alguno de sus documentos.

La naturaleza dual de los datos de navegación debería tener, a nuestro parecer, un reflejo normativo acorde con dicha situación. Si tales datos participan del doble carácter mencionado, hubiese sido más correcto que la Directiva acogiera un

único precepto relativo a los mismos. En este sentido, pensamos que la corrección sistemática exige un precepto único, en el que se recojan las soluciones relativas, no tanto a la confidencialidad de las comunicaciones en sentido genérico, lo cual puede ocasionar dudas respecto del objeto directo del precepto, sino de los datos generados en las comunicaciones electrónicas. En parte, es esta la solución que recoge el artículo 5, al referirse a las comunicaciones y a los datos de tráfico. Por ello, resulta más adecuado acoger el mantenimiento de los datos sobre tráfico, a que se refiere el artículo 6, en el texto del artículo 5, como una excepción más añadida a las que ya recoge, en atención a la naturaleza y fines de esta información. Es esta la solución que, al menos parcialmente, acoge el artículo 5.1 *in fine* de la Directiva 2002/58/CE, a diferencia del silencio que guardaba el texto de la Propuesta. De esta forma, se consagra expresamente el carácter excepcional del tratamiento de los datos sobre tráfico, en consonancia con la confidencialidad que respecto de los mismos exige el artículo 5.

Igualmente, es este el sentido que parece deducirse de la Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y del comercio electrónico. El artículo 14 del mismo, relativo a la responsabilidad de los operadores de redes y proveedores de acceso, establece lo siguiente:

> *1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de la sociedad de la información que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a sus destinatarios.*
>
> *No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.*
>
> *2. Las actividades de transmisión o provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.*

Como se puede observar, este precepto no sólo incluye los servicios de acceso, que aquí interesan, sino también los de transmisión, encaminamiento de señales, entre otros. En cualquier caso, no se observa en ningún momento la distinción entre datos de tráfico y datos de contenido, sino que tan sólo se alude a datos. Es cierto que, en aras de determinar la responsabilidad de los proveedores de acceso, alude al supuesto de los datos generados, que bien pudiera referirse a los datos de tráfico, sin embargo al hacer alusión al régimen de almacenamiento en el párrafo 2º, la referencia a los datos almacenados es general, sin especificación de su naturaleza.

Por cierto, que la solución adoptada es similar a la recogida en la normativa sobre protección de datos en las telecomunicaciones: la limitación temporal del almacenamiento, justificado éste mientras se pretenda satisfacer la finalidad a que se destinan aquéllos.

No obstante lo anterior, la LSSICE contiene una norma concreta sobre retención de datos por diversos operadores. Establece el artículo 12 de aquélla:

> *1. 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.*
>
> *2. Los datos que, en cumplimiento de lo dispuesto en el apartado anterior, deberán conservar los operadores de redes y servidores de comunicaciones electrónicas y los prestadores de acceso a redes de telecomunicaciones, serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.*
>
> *Los prestadores de servicios de alojamiento de datos deberán retener sólo aquellos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.*
>
> *En ningún caso, la obligación de retención de los datos afectará al secreto de las comunicaciones.*
>
> …
>
> *3. Los datos se conservarán para su utilización en el marco de una investigación criminal para la salvaguarda de la seguridad pública, la defensa nacional, poniéndose a disposición de los jueces y Tribunal o del Ministerio Fiscal, que así lo requieran. La comunicación de datos a la Fuerzas y Cuerpos de seguridad del estado se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales*
>
> *4. Reglamentariamente, se determinarán las categorías de datos que deberán conservarse según el tipo de servicio prestado, el plazo durante el que deberán retenerse en cada supuesto dentro del máximo previsto en este artículo, las condiciones en que deberán almacenarse, tratarse y custodiarse y la forma en que, en su caso, deberán entregarse a los órganos autorizados para su solicitud y destruirse, transcurrido el plazo de retención que proceda, salvo que fueren necesarios para éstos u otros fines previstos en la Ley.*

Este precepto resulta de gran interés. Por una parte, se establece una limitación temporal de retención. Aunque podría discutirse la duración de dicho

período, se trata de una cuestión puramente numérica, pues desde un punto de vista cualitativo las razones que justifican dicha medida son acordes con las restricciones impuestas por la normativa comunitaria. Además, se establecen limitaciones respecto de los órganos que pueden acceder a la información, otorgando únicamente la potestad directa a los órganos judiciales y al Ministerio Fiscal, mientras que los cuerpos policiales y órganos administrativos deben someterse a los preceptos de la LOPD (posibilidad contenida en las redacciones iniciales). Finalmente, determina la sola retención de datos de tráfico: la dirección IP del ordenador y el momento de la comunicación.

En relación con la retención sistemática de datos de tráfico, el Dictamen 5/2002, sobre la Declaración de los Comisarios europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de Septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones[106], recoge la preocupación de las autoridades de control de los Estados miembros respecto de esta retención sistemática por períodos de más de un año para facilitar el acceso a los datos a los organismos para aplicar la Ley, pues entienden que tanta amplitud de posibilidades no está justificada, pues estas medidas sólo deben admitirse cuando son necesarias y apropiadas en una sociedad democrática, según dispone el artículo 15 de la Directiva 95/46/CE. Así, debe haber una habilitación legal y el plazo debe ser el estrictamente necesario, sin que sea admisible su fijación *a priori* y cualesquiera que sean las circunstancias del caso.

El artículo 12 parece respetar el secreto de las comunicaciones y es muy cuidadosa en señalar la información retenida, referida únicamente a cuestiones ajenas al mensaje. Sin embargo, si no se retiene ninguna información relativa al contenido de la comunicación, ¿qué finalidad tiene la retención de los datos mencionados?. Difícilmente, el conocimiento de esta información puede determinar por sí solo la realización de actividades ilícitas: será necesario conocer los sitios visitados, las informaciones vertidas, los mensajes enviados. De esta forma, o bien no poseen ninguna virtualidad los datos retenidos para la consecución de los fines señalados en el precepto, o bien el contenido se puede conocer a partir de aquéllos. En el primer caso, la retención sería injustificada, en el segundo se estaría afectando al secreto de las comunicaciones, en contra de lo dispuesto en el artículo 12.

La imposibilidad de distinguir entre lo que es contenido de la comunicación e información sobre las características de la misma en las comunicaciones por Internet, exige que la cesión al Ministerio Fiscal y a los miembros de las Fuerzas y Cuerpos de seguridad del Estado esté refrendada por la previa autorización judicial, de conformidad con las exigencias constitucionales sobre el secreto de las comunicaciones. Como señala Manteca Valdelande, no parece lógico que a las empresas que operan en Internet se les establezcan exigencias adicionales respecto de las que no operan[107].

---

[106] 11818/02/ES/Final WP 64. *www.europa.eu.int.*

Por otra parte, la expresión de las causas que motivan la comunicación de los datos del artículo 12.2, podría haber sido más explícita, concretamente podría haber explicado de forma más precisa los supuestos que justifican tales cesiones, en vez de acudir a la manida fórmula de los conceptos jurídicos indeterminados.

En relación con la posible cesión o comunicación de los datos de tráfico a los sujetos anteriormente mencionados, debemos tener en cuenta que tal cesión solamente resulta factible si tales datos se conservan aún por los operadores de telecomunicaciones. Como ya sabemos, tal posibilidad se encuentra limitada por la legislación. En efecto, las legislaciones generales comunitaria y nacional sobre protección de datos establecen el principio de finalidad, en virtud del cual no se pueden tratar los datos para la consecución de un fin que resulte incompatible con los que inicialmente se propusieron en la recogida, a la vez que se prohíbe la conservación de éstos por un plazo superior al que se requiera para satisfacer los objetivos perseguidos al recoger los datos. El Grupo de Trabajo del artículo 29 ha sostenido que una interpretación razonable de las Directivas 95/46/CE y 2002/58/CE permite sostener que estos datos pueden conservarse por un período de 3 a 6 meses, admitiendo una ampliación de dichos plazos en los supuestos de litigio[108]. Por su parte, la Agencia Española de Protección de Datos ha sostenido que, si la factura ha sido pagada, el plazo de conservación debe ser de 3 meses y de 5 años si media impago. En caso de litigio, los datos pueden conservarse hasta la resolución definitiva[109].

Aunque la incompatibilidad de fines se puede interpretar de forma extensa, sin embargo no es admisible un resultado que elimine todas las restricciones que pretende la norma. Así, la determinación de las características de la comunicación en aras de su facturación posterior no guarda relación alguna con la investigación criminal en sentido amplio. Por otra parte, la legislación de protección de datos en el sector de las telecomunicaciones establece la prohibición de los actos de interceptación o vigilancia de las comunicaciones sin el consentimiento de los afectados, salvo autorización legal. Es decir, por una parte se establece la prohibición general de mantenimiento y uso extraño a los fines, por otra se establecen una serie de excepciones a tal regla.

---

[107] MANTECA VALDELANDE, VICTOR. *El proyecto de Ley de Internet y Comercio electrónico.* Diario La Ley, núm. 5508. 22 de Marzo de 2002. Pág. 2.

[108] GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. *Dictamen 1/2003, sobre almacenamiento de los datos de tráfico a efectos de facturación (adoptado el 29 de Enero de 2003).* 12054/02/ES. WP 69. *www.europa.eu.int.*

[109] *Informe de la Agencia Española de Protección de Datos sobre conservación de los datos de facturación telefónica.* www.agpd.es.

Respecto de dichas excepciones, el artículo 15.1 de la Directiva 2002/58 permite limitar la exigencia de la destrucción de los datos de tráfico, cuando concurra razones de protección de la seguridad nacional, la defensa, la seguridad pública, prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas. Como ha señalado el Grupo de Trabajo del artículo 29[110], del juego conjunto de los dos preceptos se deduce que los operadores de telecomunicaciones y proveedores de acceso a Internet no pueden conservar los datos de tráfico, alegando que tal medida muestra una actitud diligente con el fin de satisfacer la ley. Para admitir tal posibilidad, es necesario que concurran expresamente las circunstancias recogidas en el artículo 14. A su vez, el Tribunal Europeo de Derechos Humanos ha establecido que la alegación de algunas de las circunstancias del artículo 14 requiere que se acredite la concurrencia de una serie de presupuestos, de conformidad con el artículo 8 del Convenio europeo de protección de los Derechos Humanos y las Libertades fundamentales de 4 de Noviembre de 1950: la existencia de un fundamento jurídico, la necesidad en una sociedad democrática de realizar las escuchas y grabaciones y la adecuación de dichas actuaciones a alguno de los objetivos mencionados en el Convenio. El TEDH, para determinar los límites de los derechos humanos, ha realizado el escrutinio de estos tres criterios.

El Tribunal se ha pronunciado sobre estas cuestiones en diversas ocasiones, la mayoría de ellas respecto de las actuaciones de escucha y grabación efectuadas por los agentes de policía. En el *asunto Klass y otros contra Alemania*[111] se debatía sí la legislación alemana establecía suficientes garantías que conciliasen la injerencia en las comunicaciones con la seguridad del Estado. El Tribunal consideró que las garantías establecidas por la legislación alemana eran conformes al Convenio (existencia de indicios de infracciones graves, ausencia de todo otro medio de averiguación o dificultad extrema de los mismos y restricción de las escuchas al sospechoso y personas con quienes comunique). De esta forma, se consideraba que existía suficiente fundamento jurídico. Además, se establecía la necesidad de un control judicial y de que el interesado fuera informado una vez concluida la vigilancia, siempre que no se haga peligrar el fin de las escuchas. En el *asunto Malone contra el Reino Unido*[112], en el que se debatía la conformidad de la utilización de aparatos de registro de los números marcados y otras circunstancias de las llamadas telefónicas con el

---

110 GRUPO DE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Recomendación 3/99, sobre la conservación de los datos sobre tráfico por los proveedores de servicio de Internet a efectos de cumplimiento de la legislación.* 7 de Septiembre de 1999. 5085/99/ES/FINAL.

111 Sentencia del T.E.D.H. de 6 de Septiembre de 1978. *Série A des publications de la Cour, num. 28*.

112 Sentencia del T.E.D.H. de 2 de Agosto de 1984. *Série A des publications de la Cour,* num. 82.

artículo 8 del Convenio, el Tribunal estimó que la falta de una normativa que regulase los modos y límites de los actos de grabación suponía una violación del citado precepto, ante la falta de fundamento jurídico alguno.

En el *asunto Huvig contra Francia y asunto Kruslin contra Francia*[113], el Tribunal consideró que los límites existentes en el derecho francés no eran suficientes: no se limitaban las personas susceptibles de escucha, ni las infracciones que podían motivar aquéllas; el Juez no estaba sometido a norma alguna para fijar la duración; no se establecían condiciones de garantía respecto de las síntesis de las grabaciones. Además, las garantías existentes en Francia no derivaban de la existencia de una normativa precisa, sino, en muchas ocasiones, de la práctica judicial y administrativa. En definitiva, se observa que el TEDH exige la existencia de una serie de límites y garantías que impidan que las grabaciones y escuchas se conviertan en el ejercicio de una potestad discrecional, preventiva y general, que pueda afectar a cualquier sujeto sin que exista una justificación precisa para ello.

A este respecto, resulta bastante esclarecedora, tanto de las intenciones de los Estados como del régimen jurídico aplicable, la Resolución 3/99 del Grupo de trabajo del artículo 29, sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones[114]. Tras señalar que el objeto de la resolución es analizar las interceptaciones en sentido amplio, que acoge tanto el acceso al contenido como a los datos de configuración de las comunicaciones, analiza la Resolución del Consejo de 17 de Enero de 1995. En la misma se exige a los operadores la obligación de proporcionar a los Estados los datos descifrados que resulten de las interceptaciones (sobre llamadas, correos electrónicos, fax y datos generados en Internet), de las personas cuyas comunicaciones se han intervenido (incluso quienes no son directamente investigados) y los datos sobre localización geográfica en el caso de comunicaciones móviles. Además, se prevé la posibilidad de intercambiar este tipo de información con autoridades de Estados que no son miembros de la Unión europea (concretamente, E.E.U.U.). El Grupo de Trabajo pone de manifiesto que, no obstante el acierto de las medidas técnicas adoptadas, existen no obstante otras que aumentan las posibilidades de interceptación en contra de las garantías dispuestas por las legislaciones de los Estados miembros.

Se recuerda en la Resolución que

> *Cada interceptación de telecomunicación, entendida como el conocimiento de una tercera parte del contenido y/o de los datos asociados a las telecomunicaciones privadas entre dos o varios corresponsales, en particular los datos de tráfico vinculados a la utilización de los servicios de*

---

[113] Ambas sentencias son de 24 de Abril de 1990. *Série A des publications dela Cour, nums. 176-A y 176-B.*

[114] Adoptada el 3 de Mayo de 1999. 5005/99/def.

> *telecomunicación, constituye una violación de derecho a la intimidad de los individuos y del secreto de la correspondencia*[115]. *Sólo puede por tanto admitirse una interceptación si responde a tres requisitos fundamentales, de acuerdo con el apartado 2 del artículo 8 del Convenio europeo de protección de Derechos Humanos y de las Libertades Fundamentales de 4 de Noviembre de 1950, y de la interpretación reservada a esta disposición por el T.E.D.H.: un fundamento jurídico, la necesidad de tal medida en una sociedad democrática y la conformidad con uno de los objetivos legítimos enumerados en el Convenio.*

Tras recordar que la obligación de confidencialidad de las telecomunicaciones es el principio general y no la excepción, establece una serie de medidas que deben adoptar las regulaciones nacionales para conciliar la posibilidad de las interceptaciones con la protección de los derechos de los individuos, entre las que podemos destacar: determinación de las autoridades que permitan aquéllas y su fundamento jurídico, los fines perseguidos; cumplimiento del principio de especificidad, que exige el establecimiento de circunstancias precisas y conlleva la prohibición de la realización de interceptaciones generales, preventivas o exploratorias, en palabras del propio texto, de los datos de tráfico; información a la persona vigilada cuando sea posible; publicidad de la normativa habilitante de las interceptaciones.

Si se admitiera que los operadores y proveedores pudieran almacenar los datos de tráfico de forma indiscriminada, se estaría legitimando un tratamiento injustificado de la información de carácter personal, pues a priori no se puede saber si las partes en una comunicación son sujetos de alguna de las actividades que habilitan para la interceptación o vigilancia. La excepción al secreto de las comunicaciones requiere la existencia de poderosas razones, como la protección de los derechos de otros sujetos o la represión de actos criminales. En ningún caso se debe admitir la vulneración con fines preventivos. En caso contrario, se consagraría la posibilidad de realizar la vigilancia de las comunicaciones sin límite temporal alguno, pues tales actividades podrían tener por objeto conversaciones de personas no implicadas en alguno de los supuestos del artículo 15. Por otra parte, tampoco existiría ninguna limitación de carácter subjetivo, sino que se podrían registrar ingentes cantidades de

---

[115] Hemos subrayado las líneas anteriores por diversas razones. En primer lugar, se debe observar que la definición de interceptación que se acoge en esta Resolución coincide prácticamente con el concepto de cesión de datos de carácter personal que se recoge en la legislación sobre protección de datos general. Por lo tanto, el análisis jurídico de aquéllas debe tener en cuenta el régimen de las cesiones establecido en dicha legislación.
Además, el concepto de interceptación es aplicable con independencia de los sujetos que la realicen. De ahí que su realización requiera la fijación de una serie de límites, que configuran la excepción a la regla general. Es decir, la interceptación de las comunicaciones por los cuerpos y fuerzas de seguridad son una excepción de la regla general de prohibición, pero no constituyen un régimen paralelo.
Finalmente, debemos señalar que las afirmaciones vertidas en esta Resolución ponen de manifiesto que el secreto y la confidencialidad de las comunicaciones deben ser entendidos en sentido amplio, dado que la interceptación de los datos de tráfico es una violación de los mismos.

comunicaciones, con independencia de los sujetos participantes. Como señala el Grupo de Trabajo[116], se debe prohibir *la vigilancia general y exploratoria a gran escala*. Resulta obvio que respecto de la restricción de un derecho fundamental no es admisible tanta indefinición.

En términos similares a los manifestados por el TEDH se ha pronunciado el Tribunal Constitucional (que incluso ha mencionado en repetidas ocasiones las sentencias de aquel Tribunal). La STC 936/1996[117], en la que se admitió un recurso de amparo por violación del secreto de las comunicaciones del artículo 18.3 de la CE y del derecho a un proceso con las debidas garantías del artículo 24.2 de la misma, afirmaba que el primero de los derechos sólo puede ser limitado mediante resolución judicial que debe ser motivada (STC 86/95), porque sólo de esta forma se preserva el derecho de defensa y se puede hacer el juicio de proporcionalidad entre la medida restrictiva y la naturaleza de la infracción que se investiga.

Exige además esta sentencia que la resolución judicial que autorice la intervención debe especificar los hechos que se investigan y su tipificación penal, así como los números de teléfono y las personas cuyas conversaciones se van a intervenir, períodos y personas que las realizan. Finalmente, el control judicial de las intervenciones debe ser efectivo, lo que se extiende, en el caso resuelto por la sentencia, a la circunstancia de que la averiguación por las escuchas de nuevos hechos, posiblemente constitutivos de delito, diferentes de lo que inicialmente motivaron la intervención, requiere nueva autorización. Es decir, se adopta por el TC el principio de especificidad, que rechaza las escuchas exploratorias.

En el ATC 1994/13521[118] se niega la vulneración del derecho al secreto de las comunicaciones, ya que la intervención se llevó a cabo en virtud de resolución judicial en la que se especificaba el hecho punible de carácter grave (lo cual prueba el respeto al principio de proporcionalidad), el número intervenido y el destinatario (manifestaciones ambas del principio de especificidad)[119]. La STC 2000/126[120]

---

[116] GRUPO DE TRABAJO DEL ARTICULO 29. *Op. cit.*

[117] STC 1996/936. TC (sala 1ª), S 26-3-1996, núm. 49/96. BOE 1-4-1996. Base de datos Aranzadi.

[118] STC 1994/13521. TC 1ª sec 2ª, A 8-3-1994, núm. 79/1994. BOE 3-3-1998.

[119] En la mayoría de las sentencias, las argumentaciones del TC versaban sobre el carácter ilícito de la prueba obtenida mediante las intervenciones telefónicas, lo cual determinaba la imposibilidad de su uso en el proceso, so pena de vulnerar el derecho a un proceso con las debidas garantías (art. 24.2 CE) y la igualdad de las partes en el mismo (art. 14 CE). No obstante, esta cuestión excede de los propósitos de este trabajo. Así por ejemplo, la STC 1998/1494, de 2 de Abril, entendió que no se vulneró el derecho a la tutela judicial efectiva, dado que la prueba obtenida por la intervención telefónica no se admitió como prueba en el proceso, sin plantearse la vulneración del derecho del artículo 18.3 de la CE.

argumentó, en un supuesto de escuchas, sobre el cumplimiento del principio de proporcionalidad. Para determinar la concurrencia de este requisito, se debe atender a las circunstancias particulares del caso en el momento en que se adopta la medida. En relación con la exigencia de la proporcionalidad entre los hechos que se investigan y las medidas investigadoras, señaló el TC que la interceptación debe ser imprescindible en un doble sentido: en primer lugar, los datos averiguados deben ser relevantes en relación con la resolución del caso; en segundo, los datos no deben poder obtenerse a través de un medio menos gravoso.

Como se podrá observar, en las líneas anteriores se ha aludido al régimen jurídico de la interceptación de las comunicaciones con ocasión del estudio de la navegación por Internet. Esta doctrina se ha elaborado para la protección del derecho fundamental al secreto de las comunicaciones. En relación con éste, la jurisprudencia del Tribunal Constitucional parece requerir, como presupuesto de hecho, el intercambio de un mensaje entre emisor y receptor, rechazando aquellos supuestos de comunicación en los que una de las partes no lleva a cabo acto de ningún tipo, adoptando una posición pasiva[121]. Sobre esta base, la navegación por Internet no se puede considerar como un supuesto de comunicación que encaje en el ámbito de protección del artículo 18.3 de la Constitución.

Ahora bien, aunque es cierto que la construcción jurídica de la interceptación de las comunicaciones se ha hecho a la luz del citado derecho fundamental, sin embargo no se puede negar que las diferentes clases de procesos de comunicación que existen extramuros de aquél deben recibir una cobertura que resulte satisfactoria a los intereses en juego. En este sentido, la navegación por Internet conlleva el acceso a una información determinada, que es precisamente el objeto o contenido de aquélla, lo que a su vez genera una información sobre determinados aspectos de la personalidad del navegante.

Aunque efectivamente el término comunicación, entendido en sentido estricto, no es sinónimo de circulación de información sin más, ello no impide que la protección se alcance por otros medios, concretamente a través de los mecanismos creados a la luz del artículo 18.4 de la CE. Pues bien, tales datos también se protegen frente a su posible conocimiento injustificado, frente a su interceptación. Como hemos podido ver anteriormente, tanto de la jurisprudencia del TC y de TEDH, como

---

120 STC núm. 126/2000. TC (sala 2ª), 16-5-2000. BOE 20-6-2000. BOE de 20 de Junio de 2000, núm. 147 (suplemento).

121 Un extracto de la estructura y elementos de este derecho se puede encontrar en BELDA PEREZ-PEDRERO, ENRIQUE. *El derecho al secreto de las comunicaciones: algunos sobre su protección en las relaciones por correo electrónico. III Jornadas sobre Informática y Sociedad.* Instituto de Informática Jurídica. Facultad de Derecho. Universidad Pontificia de Comillas. 2001, Madrid. Con mayor profundidad, MARTIN MORALES, RICARDO. *El régimen constitucional del secreto de las comunicaciones.* Ed. Civitas. 1995, MADRID. Págs. 44 y ss.

de algunos documentos de los órganos comunitarios, se deduce que el objeto de protección en estos casos no es sólo el contenido directo de la comunicación, sino los datos generados por la misma. Es decir, el régimen de las interceptaciones refuerza la protección de los datos de carácter personal que brinda la legislación específica sobre la materia, a pesar de que su origen se encuentre en el secreto de las comunicaciones.

La posibilidad del tratamiento y cesión de los datos sobre tráfico depende de la posibilidad de conservación de los mismos. En relación con esta cuestión, se ha planteado cuál es el plazo de conservación idóneo. En los ordenamientos europeos no se acoge una solución única: en unos casos se establecen unos plazos diversos, en otros se equipara dicho plazo al de impugnación de la factura. También se deja a la autoridad nacional de protección de datos la determinación del plazo, según los casos. El artículo 6.2 de la Directiva 2002/58, permite la conservación durante el plazo en que pueda impugnarse la factura o exigirse el pago, apreciación ésta última que incluye el supuesto en el que sea el operador quien inicie la reclamación, no sólo el usuario. Además, en la práctica parece que existen muchos operadores medios que no tienen mucha capacidad técnica de almacenamiento[122].

En consonancia con las limitaciones señaladas anteriormente, la posibilidad de utilización de los datos cedidos para la consecución de los fines mencionados en el artículo 15 de la Directiva, se encuentra limitada de hecho por el deber de conservación temporal. En definitiva, la satisfacción de los fines de este tipo de datos, la determinación del pago, impide su almacenamiento en momentos posteriores. Aquellos objetivos no son directamente propios de los datos de tráfico, de ahí que no se pueda justificar su mantenimiento sobre la base de los mismos. Aunque efectivamente los Estados pueden establecer disposiciones que exceptúen las reglas contenidas en el artículo 6, entre ellas la destrucción de los datos sobre tráfico, sin embargo requieren para ello una serie de presupuestos precisos, según hemos visto. Es obvio que los mismos no se pueden observar de forma apriorística y general, por lo que no se podrán utilizar tales argumentos para impedir el cumplimiento generalizado de aquel deber.

Si bien la conservación de los datos de tráfico en sentido estricto está justificada en interés de los operadores y de los usuarios, no parece que la solución deba ser la misma en el supuesto de los datos de navegación. Debemos hacer esta salvedad porque, como ya se vio, se trata de datos que reciben la calificación genérica de datos sobre tráfico, aunque a nuestro entender se deban matizar tales apreciaciones, como también hemos advertido. Según establece la Directiva, la regla respecto de los datos sobre tráfico es su destrucción, salvo por razones de facturación. En la navegación por Internet se generan datos de tráfico en sentido estricto y datos sobre la navegación en sí. En Internet la información circula por paquetes, cuyas cabeceras contienen información derivada de la utilización de diversos protocolos referente a la

[122] También se prevé por este precepto la conservación de los datos de tráfico para fines de promoción comercial o prestación de servicios de valor añadido, cuando medie el consentimiento de los abonados.

dirección IP del equipo cliente, el destinatario, sitios visitados o aspectos diversos del contenido de la comunicación[123].

Como ya sabemos, la comunicación a través de Internet se realiza mediante una llamada telefónica, generalmente local, al proveedor de acceso a Internet. En este sentido, el operador que nos facilita la línea telefónica tiene derecho a la conservación de los datos sobre dicha llamada, con fines de facturación. Pero entiéndase bien: dado que la llamada se hace al proveedor, sólo las circunstancias del tráfico que genera dicha llamada se pueden almacenar: hora de comienzo y fin de la sesión, en cuanto determina la duración de la llamada, destinatario de la llamada, entre otros. Por el contrario, los datos sobre navegación no tienen que ser necesariamente almacenados por el operador, pues en nada ayudan a la concreción del coste de la llamada: sitios visitados, lo cual informa del contenido de la comunicación, actos efectuados en estos sitios, etc. La falta de una finalidad que justifique la conservación permite afirmar que los datos sobre navegación deberán destruirse una vez que la comunicación haya concluido. En realidad, al operador de telecomunicaciones sólo debe preocuparle la prestación del servicio y el consiguiente cobro, objetivos que se satisfacen plenamente mediante el control de la simple llamada. La navegación que realice el usuario una vez que ha accedido a Internet no afecta al servicio prestado, por lo que resulta injustificable que los operadores se inmiscuyan en aquélla.

Una solución similar se puede aplicar respecto de los proveedores de acceso, de servicios y sitios web[124]. En la mayoría de los casos, se trata de servicios que se prestan con ausencia de contraprestación, por lo que la finalidad del cobro para justificar la conservación de los datos sobre tráfico no existe en estos casos. En realidad, ya hemos señalado que los datos sobre navegación no tienen la naturaleza de datos sobre tráfico, por lo que no es necesario esgrimir el argumento de la falta de facturación para exigir su destrucción. No obstante, esta opinión no es compartida por muchos.

El Grupo de trabajo ha configurado la información sobre los sitios visitados como datos de tráfico[125]. Así, resulta necesario el argumento de la falta de fines de facturación para conseguir el objetivo de la confidencialidad, al evitar la

---

[123] Aunque todavía no se trata de una técnica generalizada, existe la posibilidad de cifrar o encriptar dichas cabeceras TCP/IP y sustituirlas por otras generales, frente a todos los elementos de las redes involucrados en la comunicación: es el *tunneling*. *El tratamiento automatizado y la transmisión de datos personales y económicos en la operativa bancaria. Documento técnico.* AUSBANC. Pág. 7.

[124] Existe, incluso, la posibilidad de que los encaminadores puedan recabar estos datos, ya que su función es encauzar y trasmitir las comunicaciones, por lo que es necesario que conozca determinada información. Cuestión diferente es que tal información se almacene por aquéllos.

[125] *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea (Documento de trabajo del Grupo de trabajo sobre protección de datos del artículo 29)*… Pág. 56.

conservación por las razones apuntadas[126]. Como señalamos, su naturaleza híbrida como información sobre tráfico y sobre contenido, permite llegar a la misma conclusión, pero por vías más correctas, a nuestro entender. Si los datos de navegación contienen información relativa al contenido de la comunicación, entonces se debe aplicar el artículo 5 de la Directiva, que establece la prohibición de actos de almacenamiento, grabación, vigilancia y demás sin consentimiento del usuario, salvo las excepciones antes citadas. Por lo tanto, los registros efectuados sobre datos de navegación deberían borrase al terminar la misma (quizás ni siquiera deberían llegar a realizarse, dado que incluso se prohibe la grabación).

Respecto de la captación de los datos sobre tráfico (en sentido amplio), se ha planteado la posibilidad de que la navegación se haga de modo anónimo. Sin duda, el potencial peligro de los datos sobre tráfico (también llamados transaccionales) existe cuando es posible conectar los mismos a un sujeto determinado, lo cual permite conocer los gustos, preferencias, decisiones, etc. del mismo. Hoy día existen casos en los que la conexión puede ser anónima, ya sea para proteger la Intimidad de sujetos inmersos en situaciones concretas (por ejemplo, conexiones por razones de suicidios, determinadas enfermedades, entre otros), ya sea para facilitar la libertad de expresión de personas que, de otra forma, no podrían manifestarse.

Como ha señalado el Grupo de Trabajo[127], de la misma manera que no se puede afirmar que Internet sea un caso de vacío jurídico al que no sea de aplicación las disposiciones existentes, igualmente no se puede ni se debe pretender que las restricciones que se pretenden establecer en este ámbito sean mayores que las impuestas fuera de la red. Por lo tanto, debe admitirse la posibilidad de un uso anónimo de los servicios que ofrece Internet, pues los mismos se pueden aprovechar de forma anónima fuera de ella. Así, existe un gran número de personas que navegan

---

[126] Como ya se ha dicho, los proveedores de servicios y titulares de sitios pueden percibir de los operadores de telecomunicaciones, como prima por las visitas recibidas, parte de la facturación de las llamadas efectuadas con destino a los mismos. En este sentido, se podría entender que aquéllos también están interesados en la facturación, a la vez que necesitan justificantes de las conexiones dirigidas hacia sus contenidos para exigir dicho pago. Sin embargo, en estos casos sería necesario que los usuarios fueran informados de tal posibilidad, que se deriva de las relaciones internas entre operadores proveedores, sin que en las mismas participen los usuarios. En estos casos, los sitios informan del tratamiento de los datos y acogen cláusulas de consentimiento tácito, lo que supone que se trata de información cuya conservación y tratamiento sigue las reglas generales de protección de datos, pero no las propias de los datos de tráfico, que justificarían el tratamiento por razones de facturación sin necesidad de consentimiento alguno.

[127] GRUPO DE TRABAJO SOBRE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Recomendación 3/97, sobre Anonimato en Internet.* 3 de Diciembre de 1997. XV D/5022/97 ES final. Más recientemente, *Recomendación sobre determinados requisitos mínimos para la recogida de datos en línea de datos personales en la Unión Europea.*

diariamente de forma ociosa, como si estuvieran hojeando libros o viendo escaparates. Estas actividades, fuera de la red, no implican captación de datos personales, pues no permiten alegar motivos de interés público (persecución y averiguación de actos constitutivos de delito), contractuales (necesidad de conocer la identidad del consumidor que pretende celebrar un contrato) y demás, que justifiquen tal posibilidad. Por lo tanto, debería ser posible la navegación totalmente anónima en estos casos, permitiendo la recogida de datos sólo en el supuesto de que medie consentimiento de los afectados o, al menos, facilitar el empleo de seudónimos, como ocurre, por ejemplo, en el caso de las certificaciones de la firma electrónica. Como señala Corripio Gil-Delgado, el anonimato es expresión de la libertad de expresión, del secreto de las comunicaciones y de la Autodeterminación informativa[128].

b. Supuestos de tratamiento y cesiones invisibles.

La navegación por Internet, a veces realizada de forma inocente y cándida, sin mayor pretensión que la de ocupar el tiempo satisfaciendo una curiosidad sin finalidad alguna, genera una serie de datos de carácter personal cuyo tratamiento puede ser conocido y tácitamente consentido en unos casos y desconocido en otros. No nos estamos refiriendo a la mayoría de los supuestos en los que, como ya hemos visto, la llamada telefónica al proveedor de acceso y la posterior navegación, crean una serie de registros sobre la duración, desconexión, sitios visitados, etc. Un gran número de usuarios desconoce que la información que generan se almacena con diversos fines. Más bien, pretendemos ahora analizar aquellos casos en los que los datos que se generan no solamente se captan por parte de los distintos agentes de forma directa o indirecta, cuando éstos últimos guardan alguna relación con el navegante, sino que además son conocidos por sujetos cuya intervención desconocemos porque se realiza de manera invisible, sin que se sepa en ningún momento (salvo curiosidad de los afectados, lo cual no es muy probable) que se ha contactado, en mayor o menor medida, con tales sujetos.

Si se desconoce esta posibilidad, difícilmente se puede tener una voluntad de control sobre los datos. Por esta razón, entendemos que esta cuestión merece un estudio separado. Las captaciones y tratamientos invisibles son posibles debido al elevado nivel técnico que ha alcanzado el software que se utiliza en relación con la red.

b.1. Los hipervínculos.

Un primer supuesto de estos tratamientos es el de los llamados hipervínculos invisibles. En este caso, se trata de una posibilidad que se obtiene por el uso de los programas de navegación conocidos. En efecto, estos programas permiten

---

[128] CORRIPIO GIL-DELGADO, MARIA DE LOS REYES. *La protección de datos personales en Internet.* Boletín del Ministerio de Justicia… Pág. 2924.

que se pueda incluir en la página, mediante un orden HTML[129], un vínculo que enlaza con otra página, para descargar imágenes. No es necesario que estas imágenes se encuentren recogidas en la página en la que se inserta el vínculo. Estos vínculos invisibles son muy utilizados en el ámbito del marketing y la publicidad, pues los mismos permiten que las empresas de dichos sectores incluyan *banners* o pancartas de publicidad en las páginas a las que acceden los usuarios[130]. Tal inclusión de publicidad se realiza en virtud de acuerdos que dichas empresas tienen con el proveedor de servicios que aloja las páginas donde se inserta el contenido publicitario.

Uno de los casos más conocidos es el de Double Click. Cuando un usuario desea visitar un sitio que se encuentra adherido al sistema Double Click, obtiene en su equipo el contenido de la página acompañado de un espacio que se reserva a la inclusión de un contenido publicitario (lo que se denomina en terminología de Internet *banner*). Tal circunstancia se comunica por el navegador a los servidores de Double Click. Una vez que se ha recibido la página, el navegador solicita de Double Click la inclusión de uno de los múltiples contenidos publicitarios que posee, en función de las características del usuario ya conocidas, pues el navegador remite un a serie de datos en la llamada *cabecera http* (en la información que se remite al solicitar el acceso a un sitio en la red, la primera parte de esta solicitud contiene la información sobre características del equipo, software, etc. ya señalados). Tales datos son registrados por esta empresa en su base de datos, mediante la adjudicación de un número de identificación único, y tratados en cada visita que el usuario realiza a páginas adheridas a la misma. Tal base de datos es actualizada de forma continua, lo cual permite personalizar los contenidos publicitarios enviados[131]. Double Click ha afirmado que los datos incluidos en sus ficheros son anonimizados previamente y que, lógicamente, los mismos no son cedidos de forma nominativa a sus anunciantes. La recogida de datos personales también se realiza mediante el empleo de cookies, como veremos más adelante.

La importancia de la recogida de estos datos supera los fines meramente publicitarios. Efectivamente, los ficheros de datos recabados permiten la obtención de ingresos a consecuencia de la venta a terceros de los mismos, lo que supone una

---

[129] El código de una página web es el conjunto de órdenes que configuran dicha página. Tal código se elabora mediante el uso de HTML, un lenguaje de programación muy utilizado en la elaboración de páginas.

[130] Las empresas publicitarias saben la página a la que deben enviar el contenido publicitario porque en el código HTML de la página visitada se incluye la orden HTTP_REFERER, que permite conocer la página de referencia, es decir, la página a la que se debe enviar la publicidad.

[131] Sobre estas cuestiones y otras relacionadas con otras empresas que llevan a cabo experiencias parecidas de tratamiento de datos, GAUTHRONET, SERGE y NATHAN, FREDERIC. *Les services en ligne et la protection des données et de la vie privée. Etude pour la Commission del Communautés Européennes (DG XV).* Págs. 91 y ss. Este trabajo se puede encontrar en http://www.europa.eu.int/.

cesión de datos. A pesar de la declaración de intenciones manifestada por sus dirigentes, AOL (America Online), el mayor proveedor de acceso y servicios de los E.E.U.U., ha comercializado ficheros nominativos de datos de sus abonados. Generalmente se trata de ficheros cedidos a empresas de medios de comunicación (sobre todo, televisión por cable), los cuales se elaboran en función de unos criterios predeterminados: por ejemplo, la realización de compras en línea. Para completar la información de tales ficheros, se accede a otras bases de datos pertenecientes a empresas de marketing. La comercialización se realiza a través de un broker especializado en ventas de ficheros. Como se puede observar, se trata de información que pasa por muchas manos, que es objeto de múltiples cesiones, sin que tales extremos hayan sido reconocidos. Incluso se han llegado a ceder los números de teléfono de los abonados, pues AOL tiene los datos de facturación y navegación de todos ellos, para unas finalidades estrictas claro está, entre las que no parecen encontrarse tales cesiones[132].

En otro orden de cosas, de la exposición anterior se deduce que el titular de la página o sitio que el usuario visita ha cedido los datos a la empresa de publicidad. El titular de la página que se visita ha configurado la misma de forma que, cuando se visite la misma y se obtengan una serie de datos de navegación, éstos se transmitan al titular de la página que remite la publicidad. A la vez que se activa el vínculo que conecta con la página de la empresa de publicidad, el navegador envía a la misma la siguiente información, que previamente ha remitido al servidor que alberga la página: dirección IP del usuario, página remitente (como ya se ha visto), configuración del navegador del usuario (marca, versión, idioma), sistema operativo del equipo cliente; artículos de prensa leídos en la página (en el caso de que así sea). En definitiva, se trata de información que permite esbozar un perfil del usuario[133].

Se deduce de todo lo anterior la concurrencia de una sola voluntad, la del titular del sitio visitado, adoptada de forma apriorística y que se ejecuta de automáticamente, dadas las posibilidades técnicas. Es obvio que no existe voluntad

---

[132] GAUTHRONET, SERGE y NATHAN, FREDERIC. *Op. cit.* Págs. 123-124.

[133] En muchos casos, tal información se ve completada por la que, de forma voluntaria, presta el propio usuario a través de los formularios propuestos en las páginas. No podemos olvidar el enorme valor económico que tales datos tienen para las empresas de marketing, las cuales se ahorran los elevados costes de la prospección. Por si fuera poco, los sitios publicitarios también captan gran cantidad de datos a través de la inserción de cookies y de las órdenes de búsqueda de páginas dirigidas al navegador (*charloteo del navegador).* Tal profusión de fuentes proporciona además un alto grado de fiabilidad respecto de los datos recabados.
Quizás se podría pensar que la información mencionada no reviste carácter personal, pues hace referencia a circunstancias que no están, en principio, conectadas a una persona determinada. Nada más lejos de la realidad. En muchos casos, los formularios indican de forma directa quien es el navegante. En otros, la falta de éstos últimos no elimina la calificación de la información como personal, pues es posible que la persona, aunque no identificada, sea identificable. Los medios técnicos empleados pueden recabar una y otra vez datos que permitan la identificación directa o indirecta de quien navega.

alguna del usuario que accede a la página que alberga el hipervínculo invisible en tal sentido: si fuera consultado, en muchas ocasiones rechazaría el envío de dicha publicidad.

En este sentido, resulta claro que en estos casos se está produciendo una cesión o comunicación inconsentida de los datos de carácter personal recogidos, desde la página visitada a la página publicitaria. Podría discutirse si la recogida de los datos se ha efectuado con el consentimiento de los usuarios (pues en muchas ocasiones existen cláusulas relativas a la protección de los datos recabados, aunque en la mayoría de estos se trata de los datos expresamente solicitados, no de los generados por la mera navegación). Pero de lo que no hay ninguna duda es que el usuario que observa la publicidad que se inserta en la página que visita, en ningún momento ha podido prestar su consentimiento a la cesión, pues es desconocedor de que la misma se ha producido: difícilmente se puede autorizar lo que no se sabe que se ha producido o se va a producir. Tal conclusión resulta incompatible con la legislación general sobre protección de datos, que como ya hemos visto al estudiar el régimen general de la cesión, exige consentimiento del afectado (artículo 11 de la LOPD, así como la Directiva 95/46 establece la regla general de la exigencia de consentimiento para el tratamiento de datos en el artículo 7 a), lo que se extiende, por supuesto a la cesión).

A este respecto y en cumplimiento de la normativa aplicable, el Grupo de trabajo ha adoptado la Resolución 1/99, sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software y hardware*[134]. Este documento parte de la necesidad de información al usuario de los posibles tratamientos que se van a efectuar respecto de sus datos, ante las facilidades que para dicho tratamiento proporcionan los equipos y sistemas actuales. Así, el Grupo de trabajo señala que se debe proporcionar la información al respecto, se debe informar de los vínculos que se envían desde cualquier sitio, visitado o no, así como de la información que, como consecuencia del mismo, se pretende remitir; también se debe establecer una configuración que permita a los usuarios acceder en un momento posterior a los datos que ya se han transferido.

Difícilmente se puede estar en contra de tales afirmaciones, que acogen las soluciones adoptadas por la legislación comunitaria e interna. No desconocemos el hecho de que los programas de navegación son fabricados por empresas ajenas al ámbito comunitario y que muchas páginas y servidores que las contienen, también se ubican en territorio extracomunitario (concretamente, E.E.U.U.). No obstante lo anterior, no es justificable la permisividad de los países comunitarios respecto de estas prácticas[135].

---

[134] Aprobada por el Grupo de trabajo el 23 de Febrero de 1999. 5093/98/ES/final.

[135] En relación con esto último, algunos autores han observado que los textos de condiciones generales de contratación ofrecidos por algunas empresas a los usuarios norteamericanos ofrecen un régimen de protección mayor que en el caso de la redacción europea. GAUTHRONET, SERGE y NATHAN, FREDERIC. *Op. cit.* Pág. 120.

b.2. Tratamientos y cesiones por empresas de servicios estadísticos.

Otro supuesto de tratamiento y cesión de datos desconocida por los usuarios es aquélla que se realiza a favor de una empresa de servicios estadísticos o para la realización de estudios de esta naturaleza. Estas empresas analizan dichos datos con el fin de realizar estudios sobre los hábitos de los usuarios de Internet, que después venden a los proveedores de servicios y titulares de sitios web. Se trata, por tanto, de una herramienta de planificación y adecuación del producto a las demandas de mercado. La finalidad puramente estadística de estas cesiones adelanta cual puede ser la solución al respecto. En realidad, los datos cedidos son disociados o anonimizados, agregados en terminología técnica. De esta forma, siempre que se observe esta circunstancia, no será de aplicación la legislación sobre protección de datos[136].

El Grupo de Trabajo entiende que, aún el caso de que los datos no estén disociados, sólo será de aplicación la legislación de protección de datos general, no la normativa especial del sector de las telecomunicaciones. Argumenta el Grupo que tales actividades no suponen en ningún caso transmisión o encaminamiento de señales en la red (presupuestos de aplicación de tal normativa), no adoptan función alguna que permita o facilite la conexión entre el usuario y el sitio visitado. No podemos negar que la participación de estas entidades no se hace por motivos de la comunicación, es decir, no tiene como finalidad última la conexión en sí. Por otra parte, la definición de transmisión de señales que acoge la regulación comunitaria, hace referencia al concepto de transporte de dicha señal. Así, los actos aquí analizados no se incluyen en dicha definición, pues aunque ocasionan transmisión, ninguno de los sujetos que la generan actúa como portador de aquélla. Debemos tener en cuenta que la cesión de tales datos podría realizarse por cauces distintos a las redes de telecomunicaciones, por lo que la participación de la misma, en estos casos, no implica especialidad alguna que justifique la aplicación de la normativa sectorial.

b.3. El *software* de control.

Otro supuesto de posible cesión y consiguiente tratamiento de datos que se plantea con ocasión de la navegación por Internet es el relativo a la transmisión de datos de carácter personal motivada por la utilización del llamado *software de control.*

---

[136] Es cierto que el artículo 2 de la LOPD establece que los datos tratados con fines estadísticos se someten a su legislación y, en su caso, a los preceptos de aquélla. Sin embargo, si los datos están disociados, de forma que no se pueden conectar a una persona identificada o identificable, conforme se deduce del artículo 3 f), entonces la información no reviste el carácter de personal, según la letra a) del mismo artículo 3.

Como vamos a ver, se trata de una de las manifestaciones de posibles abusos de los datos de carácter personal motivados por el elevado nivel técnico que se ha alcanzado en el ámbito de Internet. Estas aplicaciones también han recibido la denominación de aplicaciones E.T., porque llevan a cabo una función similar a la actividad que deseaba realizar el popular personaje de la película que lleva su nombre: *"una vez que se han instalado en el ordenador del usuario y han aprendido lo que querían saber, hacen lo mismo que el extraterrestre de Steven Spielberg: llamar a casa"*[137]. El autor del citado artículo, que se reproduce en parte por el Grupo de Trabajo en su informe general sobre la materia, recoge varios supuestos de este software. Veamos alguno de ellos.

Surfmonkey en un software que evita las conexiones de menores a sitios no apropiados a los mismos. Tras este fin, positivo sin duda, del programa, la utilización del mismo conlleva la remisión a su página de información sobre la navegación efectuada por los menores: número de identificación personal (si se utiliza), número de teléfono y dirección de correo electrónico. Microsoft también creó un software similar, que se incluía en el sistema operativo Windows 95. Al registrarse el usuario en la página de Microsoft, enviaba información sobre otros programas instalados en el disco duro, a la vez que gozaba de los datos voluntariamente prestados en el cuestionario de registro. Parecidos fines tiene el programa RealJukebox, de la empresa Real Networks. Se trata de una aplicación que sirve para la descarga de ficheros de audio desde la red o desde un CD, para escucharlos en el ordenador. Según se deduce de un análisis de este programa, cada vez que el usuario pretende escuchar música en su equipo, remite información sobre su elección y su dirección IP a la página de Real.

Otro caso de software E.T. es Radiate[138]. Se trata de una empresa publicitaria que insertaba en diversas páginas anuncios que incluían dichos programas, lo que permitía a Radiate conocer los anuncios que los usuarios habían visitado. Se trata de alguno de los muchos casos de tratamiento invisible de datos a través de programas que se instalan en los equipos clientes sin que los usuarios tengan noticia de tal extremo. En realidad, se trata de una práctica relativamente extendida en las empresas que aparecen en Internet, dado que permite recabar datos de gran utilidad comercial por el mínimo coste del material informático. No obstante, debemos plantearnos, en estos casos, si estamos o no ante cesiones de datos o por el contrario son más bien supuestos de recogida.

El artículo 3 de la LOPD, como ya sabemos, define la cesión como *toda revelación de datos realizada a persona distinta del interesado*. De lo anterior se deduce indirectamente que se trata de aquellos actos en los que la persona que previamente ha recabado los mismos del interesado o afectado, los transmite o simplemente muestra a

---

137 ADAM COHEN. *Spies among us*. Time Europe. July 31, 2000. Vol. 156, núm. 5.

138 *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea (Documento de trabajo del Grupo de trabajo sobre protección de datos del artículo 29)*… Pág. 51.

un tercero con posterioridad. El software de control recoge la información del ordenador del usuario y la transmite a la página de quien ha instalado dichos programas, es decir, sólo intervienen dos sujetos: el usuario titular de los datos y la empresa que, a través de la instalación *silenciosa* del programa *capta* los datos. En realidad, nos encontramos ante actos de recogida de datos, no ante cesiones, pues no participa intermediario alguno que recoja aquéllos y los ceda a un tercero que no tiene relación inicial con los afectados. El programa no es un sujeto diferente de su titular, sino que éste lo ha introducido en el equipo con fines de recogida. Por supuesto, se trata de situaciones que merecen toda la atención y protección posibles, pero no la propia de las cesiones de datos, pues no revisten tal naturaleza.

b.4. Las *cookies*.

Diferentes problemas, a nuestro entender, pueden plantear las *cookies*, aunque también puedan ser estudiadas como caso de tratamiento invisible. Las cookies son ficheros de datos que se generan en el ordenador del usuario que navega por Internet, en un directorio del mismo. Son creados por los servidores web (proveedores de servicios), que los envían al programa de navegación que el usuario tiene instalado en su equipo, con la intención de recoger posteriormente la información que, sobre el equipo y, en muchos casos, sobre el usuario, se ha agrupado en dicho fichero. Tales ficheros recogen información sobre los sitios visitados por el usuario, anuncios, compras o adquisiciones realizadas, etc. Se trata, por tanto, de la huella electrónica que vamos dejando a la vez que navegamos por diferentes sitios en la red. Como se puede comprobar, tal herramienta posee un gran valor para los servidores y los sitios web, que gozan de un medio fidedigno para conocer los gustos, preferencias, decisiones y demás de los usuarios[139]. No obstante, la función de las cookies no se queda en la captación de dicha información, que por otra parte pudiera ser meramente estadística, sino que en muchos casos permite conectar la misma a la persona a quien pertenece[140].

---

[139] Por estas razones, el empleo de las cookies es general. Todos los servidores utilizan este medio para conocer los hábitos y así poder ofrecer publicidad personalizada, bienes o servicios por los que el usuario ha manifestado su preferencia en algún momento. Estas y otras posibilidades superan las estrictas finalidades estadísticas, dado que permiten un acercamiento a la demanda, no de modo indiciario, sino directo.

[140] No obstante lo anterior, tampoco se puede dejar de reconocer que las cookies también poseen indudables ventajas. Quizás la más patente, que es además la que inicialmente justificó su existencia, sea la de facilitar o agilizar la navegación. En efecto, la instalación de las cookies remitidas por los servidores en los ordenadores de los usuarios permite una conexión con la página en cuestión más rápida, dada la información que sobre la misma se ha almacenado previamente. Por otra parte, los usuarios pueden encontrar un beneficio en el hecho de que las cookies permiten también personalizar la oferta de la página visitada, dado que las cookies permiten conocer previamente las tendencias del usuario.

La Agencia Española de Protección de Datos ha proporcionado una definición de las cookies. Según aquélla, se entiende por cookies *el conjunto de datos que envía un servidor Web a cualquier navegador que le visita, con información sobre la utilización que se ha hecho, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. Esta información se almacena en un fichero en el directorio del navegador para ser utilizada en una próxima visita a dicho servidor*[141]. Quizás se podría pensar que las cookies no afectan en nada a la protección de datos de carácter personal, pues la información que recaban de los equipos clientes no hace necesariamente referencia a ninguna persona identificada o identificable. Sin embargo, tal afirmación no se puede hacer de manera categórica: en algunos casos, la información en cuestión no es de naturaleza personal, sin embargo en otros sí. Es más, nos atreveríamos a decir que, dadas las posibilidades técnicas, en la mayoría de los casos la información que se obtiene permite conocer al sujeto directamente o, cuando menos, lo hace identificable. Veámoslo de manera detenida.

En el momento en que un usuario desea conectarse a la red, el servidor que le proporciona el acceso le asigna una dirección IP, es decir, un número de identificación, el cual se incluye dentro de la información que las cookies captan a favor del servidor. En el supuesto de acceso a través de un modem[142], la dirección IP asignada es dinámica, es decir, varía de una sesión o conexión a otra. De esta forma, un mismo número, asignado a un usuario y recuperado cuando éste se desconecta, puede otorgarse en el día a diversos usuarios. Como se puede observar, se trata de tener un control del usuario conectado solamente para la sesión en curso, pues una vez terminada la misma se asigna dicha dirección a otro equipo[143]. Podríamos pensar, por tanto, que la configuración dinámica de la dirección IP impide la identificación del usuario, lo que eliminaría la necesidad de aplicar la normativa sobre protección de datos[144]. Sin embargo, tal afirmación no se puede sostener rotundamente.

---

141 AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Recomendaciones a usuarios de Internet.* MADRID, 1997. Se puede encontrar esta publicación en la Memoria de 1997, Anexo IV.

142 El modem (vocablo resultante de la fusión de los términos modulador y demodulador) es un aparato que permite la conexión del ordenador a la línea telefónica, de forma que desde éste se pueda transmitir información, así como recibirla, mediante la realización de una llamada telefónica. Es un adaptador del equipo a la línea mediante la conversión de las señales digitales en frecuencias de audio.

143 Tal circunstancia no quiere decir, no obstante, que no exista posibilidad de control, sobre una conexión determinada. Por el contrario, la información de la misma, concretamente la dirección IP utilizada, se almacena *temporalmente* en el archivo *log* del servidor, lo cual se podría utilizar, por ejemplo, por razones de investigación criminal.

144 En este sentido, RIBAS ALEJANDRO, JAVIER. *Aspectos jurídicos del uso de las cookies.* http://www.onnet.es/.

En muchas de las páginas visitadas, los usuarios, con la intención de obtener algunos servicios (no necesariamente de transacción comercial, pues en tal caso la identificación del usuario demandante del bien o servicio sería necesaria por razones obvias), rellenan unos formularios con información personal: nombre, domicilio, sexo, profesión, dirección de correo electrónico, etc. (alguno de estos datos deben prestarse obligatoriamente, otros no). En tal caso, el servidor tiene conocimiento de quien es la persona a quien se ha asignado tal dirección IP. Claro está que el usuario tiene la posibilidad, como de hecho ocurre, de proporcionar información falsa, pero también existe la posibilidad contraria. No obstante lo anterior, en la mayoría de los casos, la oferta de dichos formularios va acompañada de una cláusula sobre protección de datos, de la que se deduce que la contestación a los mismos implica el consentimiento tácito para el tratamiento y la cesión de los datos que se han ofrecido[145]. En este mismo sentido se manifiesta Munar Bernat, para quien la dirección IP es un dato de carácter personal desde el momento en que el proveedor de acceso u otros operadores de la red tienen la posibilidad de identificar a la persona que está detrás del ordenador. A tal efecto, reproduce este autor una normativa belga que permite a los jueces acceder a dicha identificación, estableciendo la correlativa obligación de posibilidad de identificación a los proveedores de servicio[146].

A lo anterior, debemos añadir que precisamente una de las funciones que tienen las cookies es poder eliminar la mayor o menor indeterminación que las direcciones IP dinámicas pudieren suponer respecto de la identificación del usuario. Generalmente las cookies contienen un número identificador único, que lógicamente se conecta con la información que se recoge en aquéllas. De esta forma, se eliminan gran parte de los problemas de indeterminación de las direcciones IP dinámicas. Es

---

No obstante, con el fin de que las direcciones IP puedan proporcionar alguna información sobre las conexiones realizadas, los servidores asignan un número multiplicador a cada dirección, el cual refleja aproximadamente la cantidad de conexiones que se corresponden con cada dirección utilizada diariamente. Sobre estas cuestiones, RAMOS SUAREZ, FERNANDO. *¿Es legal el uso de las cookies?*. REDI (Revista electrónica de Derecho Informático). http//:v2.vlex.com/global/redi.
También sobre estas cuestiones, RUIZ MIGUEL, CARLOS. *Protección de datos personales y comercio electrónico.* En *Comercio electrónico en Internet.* GOMEZ SEGADE, JOSE ANTONIO, FERNANDEZ-ALBOR BALTAR, ANGEL y TATO PLAZA, ANXO (coords.) Ed. Marcial Pons. MADRID, 2001. Pág. 408-409.

145 A este respecto, resulta sorprendente las diferencias que se observan en cuanto al volumen de los datos que se solicitan en unos sitios y los que piden en otros. La enorme diferencia en algunos casos nos obliga a plantearnos sobre la cantidad que deben recabar para satisfacer los fines exclusivos de la prestación del servicio ofrecido.

146 MUNAR BERNAT, PEDRO A. *Protección de datos en el comercio electrónico.* En *Comercio electrónico y protección de los consumidores.* Coord. BOTANA GARCIA, GEMA ALEJANDRA. Ed. La Ley. MADRID, 2001. Pág. 281.

decir, aunque el usuario se desconecte y se vuelva a conectar, lo que supone la atribución para la nueva sesión de una nueva dirección IP, sin embargo si navega al mismo sitio que en sesiones anteriores, el servidor conocerá el equipo por el identificador que contienen las cookies[147]. Además, como señala Llaneza González, las IP dinámicas evitan la identificación por los servidores de las páginas visitadas, no así por el proveedor de acceso[148].

No obstante, no es esta la única solución adoptada respecto de la identificación en las sesiones de navegación. Existen muchos supuestos en los que la dirección IP asignada a los usuarios es fija, es decir, es la misma para todas las sesiones. Por ejemplo, las direcciones IP fijas se otorgan, hasta la fecha, a los usuarios que navegan mediante una conexión por el sistema ADSL, o los que navegan mediante la utilización de teléfonos móviles[149]. En estos casos, se identifica perfectamente el equipo desde el que se realizan dichas conexiones, las decisiones y preferencias que manifiesta en su navegación el usuario de dicho equipo, máxime si tenemos en cuenta la posibilidad de los formularios (aunque en este caso media consentimiento, como ya hemos señalado). Sin embargo, las posibilidades de identificación, hasta este momento, son indirectas, es decir, permiten que la persona titular de los datos sea identificada. Se trata de una persona identificable. Tal circunstancia es suficiente para determinar la aplicación de la normativa sobre protección de datos, como se deduce de la definición ya apuntada de datos de carácter persona. Sin embargo, las posibilidades que tales medios ofrecen van más allá de la mera *identificabilidad* del usuario: en realidad, permiten la plena identificación de dicho sujeto.

---

147 No obstante, debemos tener en cuenta que la información recogida a través de las cookies no es accesible a cualquier servidor, sino que únicamente se puede conocer aquélla por quien ha insertado las mismas en el equipo cliente. Toda posibilidad de cesión de datos a través de la red, mediante su revelación a otros servidores, está vetada, sin perjuicio de que las mismas puedan realizarse fuera de Internet por medios tradicionales, lo cual entraría dentro del ámbito del régimen general de las cesiones.

148 LLANEZA GONZALEZ, PALOMA. *Internet y comunicaciones digitales*. Ed. Bosch. BARCELONA, 2000. Pág. 267.

149 El ADSL (Asymmetric Digital Subscriber Line) es un sistema o modo de conexión a red, que representa mayores ventajas que una conexión normal por modem. El ADSL supone la utilización de la Red Digital de Servicios Integrados (RDSI), lo cual permite una velocidad de transmisión, al menos teórica, de 128 K a 1 M de información, según el ancho de banda contratado y de la dirección de la transmisión (envío o recepción de la información). También tiene la ventaja de que el modem utilizado es un *splitter* o discriminador, de forma que con una sola línea telefónica podemos navegar y realizar o recibir llamadas telefónicas de forma simultánea. Además, el atractivo práctico de este sistema radica en que su instalación va acompañada de la concesión de un tarifa plana real, es decir, de uso las 24 horas del día, a diferencia de las tarifas que se ofrecen de modo general con una conexión por modem (las llamadas tarifas onduladas, en su pago permite conexiones sin más costes durante unas horas al día).

Aunque es cierto que existe la posibilidad de adquirir un modem de conexión ADSL de forma libre, sin embargo en la inmensa mayoría de los casos tales servicios se obtienen a través de un contrato con un proveedor de servicios de Internet. Pues bien, en dicho contrato el acceso se ofrece, lógicamente, por la misma empresa que proporciona el sistema ADSL. Ello implica que la entidad que nos instala este sistema, mediante un contrato en el que se recogen los datos del usuario, es la misma que, al brindarnos el acceso, nos proporciona la dirección IP fija. De esta forma, dicha entidad conoce perfectamente que las conexiones realizadas desde un equipo (sobre todo, si pertenece a persona física) se realizan por una persona determinada e identificada, al menos por un grupo reducido de personas, lo que le permite poder identificar al usuario concreto. Es cierto que el contrato de suscripción del servicio contiene una cláusula sobre tratamiento de los datos, pero está viene referida a los que el usuario incluye en el contrato en sí, no a los que se generan como consecuencia de la navegación.

No obstante lo anterior, no debemos señalar que parte de los problemas generados se eliminan con el otorgamiento a los usuarios de ADSL de IP´s dinámicas, que se modifican con cada sesión.

La identificación del usuario es prácticamente total cuando la conexión se realiza desde un equipo móvil. Se trata de teléfonos que son de uso personal, a los que, en la mayoría de los casos, no tienen acceso otra persona que no sea el abonado. A lo anterior, debemos unir la posibilidad de ubicación geográfica del abonado en el momento de la llamada, lo cual plantea otra serie de problemas, como ya vimos.

Otra posibilidad de captación de datos de carácter personal mediante la cookies se produce en los casos de personalización del software que se incluye en los equipos de los usuarios. En efecto, gran parte del software, principalmente los sistemas operativos y los programas de navegación, permiten a los usuarios rellenar unos formularios con sus datos personales. Según los propietarios de los programas, se trata de que los usuarios se registren con el fin de obtener posteriores ventajas: actualizaciones, resolución de problemas, etc. Pero claro está, la utilización conjunta de estos datos con los obtenidos mediante el uso de cookies, permitiría de nuevo conseguir la identificación y el perfil de dicho usuario. Debemos tener en cuenta que muchos de los posibles usos que se vayan a hacer de esta información no han sido previstos en la cláusula de protección de datos del formulario, por lo que tales usos serán en muchos casos desconocidos y no consentidos, por tanto. Además, las cláusulas incluidas contienen, en ocasiones, una redacción vaga, que resulta contraria a la exigencia de una información previa y precisa, entre otros caracteres, de los fines a los que se vayan a destinar los datos, según establece el artículo 5.1 de la LOPD.

Los programas de navegación por Internet pueden ser decisivos a la hora de establecer un régimen de protección de datos de carácter personal de los usuarios. Tales programas presentan una serie de opciones que determinan dicho grado de

protección. Concretamente, la configuración de los mismos se puede realizar de manera que las cookies enviadas por los servidores no se instalen en los equipos clientes, o al menos que tal instalación se realice previa consulta al usuario de dichos equipos. Sin embargo, la configuración por defecto de los mismos, es decir, la que tienen previamente establecida por el fabricante, implica la aceptación sin consulta previa de las cookies. El Grupo de Trabajo ha señalado que, en aplicación de la normativa sobre protección de datos, la configuración por defecto de los navegadores no debería permitir la recogida de información, o al menos, solamente debería recabar aquellos datos que sean estrictamente necesarios para establecer la conexión[150].

El alto grado de desconocimiento de tales posibilidades por gran parte de los usuarios implica, en la práctica, la instalación invisible de las cookies. Difícilmente éstos últimos pueden prestar su consentimiento a una circunstancia que desconocen, pues tal posibilidad técnica no se especifica claramente en las condiciones generales del contrato de adquisición del programa de navegación. Incluso en el supuesto de que el usuario configurase el navegador para que le solicitase consentimiento sobre la admisión de las cookies, tal voluntad tan sólo cubriría la recogida de los datos a través de aquéllas. Pero como muy bien advierte Ramos Suárez[151], ello no implica consentimiento alguno al posterior tratamiento de tal información, pues en ningún momento se reclama de modo inequívoco, en la solicitud que aparece en pantalla, consentimiento para dichos tratamientos. Tampoco podemos dejar de recordar que la ignorancia sobre estas cuestiones de la generalidad de los usuarios, debería verse compensada con una redacción lo más inteligible posible de los mensajes sobre envío de cookies. En este sentido debemos recordar que el consentimiento exigido para el tratamiento de los datos debe ser inequívoco (artículo 6 de la LOPD), es decir, que no quepa dudas acerca de su existencia. Tal circunstancia no se puede acreditar cuando no ha existido solicitud a este respecto, además de que no ha existido la información previa que el artículo 5 de la LOPD exige al recabar los datos respecto de los fines para los que van a ser tratados[152].

---

[150] GRUPO DE TRABAJO SOBRE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Resolución 1/99, sobre tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware* (23 de febrero de 1999). 5093/98/ES/final.

[151] RAMOS SUAREZ, FERNANDO. *¿Es legal el uso de las cookies?...*

[152] Como se puede observar, en todas estas cuestiones resulta decisiva la divulgación de información a los usuarios, que les permita ser conscientes de su situación y de sus posibilidades. En este sentido, sería bastante conveniente establecer un régimen de obligaciones de información por parte de los intervinientes en la navegación: servidores, sitios web, etc. De esta forma, se posibilitaría a los usuarios la toma de decisiones libres y conscientes. No obstante, el requisito de la libertad puede verse mermado en aquellos supuestos, numerosos por otra parte, en que los servidores exigen como condición a los usuarios la aceptación de las cookies para poder acceder a la página que se desea visitar.

Tales extremos han sido igualmente denunciados por el Grupo de Trabajo[153]. Según dicho órgano,

> *…- En el caso de cookies, debería informarse al usuario cuando está previsto que el software de Internet reciba, almacene o envíe una cookie. El mensaje debería especificar, en un lenguaje normalmente comprensible, qué información se pretende almacenar en la cookie y con qué objetivo, así como el período de validez de la cookie[154].*

Se trata, como ya se señaló anteriormente, de exigir exclusivamente el cumplimiento de la normativa existente, cuyo régimen no distingue entre los medios de captación de información, sino que establece con carácter general, tanto la necesidad de consentimiento de los usuarios como la obligación de la información previa. En definitiva, se trata de preservar el derecho a la Autodeterminación informativa, como pilar básico de la protección de los datos de carácter personal, lo que implica la necesidad de una información clara sobre el fin y uso de las cookies y, por supuesto, de un consentimiento inequívoco como única forma de control del afectado sobre sus propios datos. Como extensión de este requisito, la Resolución 1/99 del Grupo de Trabajo, antes citada, exige además que los usuarios tengan la posibilidad de poder solicitar la eliminación de los datos, la posibilidad de ejercer el derecho de cancelación, reconocido expresamente por la Ley. Una conclusión general que se puede extraer a la luz de lo expuesto es el alto grado de incumplimiento de la legislación sobre protección de datos que se produce en Internet. Incluso, algún autor ha señalado que las cookies son ilegales e inconstitucionales, pues e parte de la base de que su configuración técnica hace que las mismas sean, de por sí, un instrumento de vulneración de los derechos de los usuarios de la red: se aceptan por defecto, se pueden vender por los servidores a diferentes empresas, se vincula, en muchas ocasiones, la visualización de la página a la aceptación de las mismas[155].

La exigencia del consentimiento en el tratamiento y cesión o comunicación de los datos captados por las cookies sólo se exceptúa en los supuestos

---

153 GRUPO DE TRABAJO SOBRE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Resolución 1/99*…

154 Microsoft ha anunciado recientemente que la nueva versión del sistema operativo Windows iba a incluir una versión beta de un programa de gestión de cookies más adecuado a los requerimientos jurídicos. Concretamente, se afirmaba que tal aplicación permitiría distinguir entre cookies provenientes de los servidores con quienes se ha conectado y las procedentes de terceros con fines generalmente publicitarios (ya vistas antes). También se señalaba que la configuración por defecto avisaría al usuario sobre la instalación de cookies y que se podrían eliminar las mismas mediante un sencillo click. Aunque se trata de un adelanto, sin embargo parece que ser persigue más bien la protección respecto de las cookies de terceros, no respecto de los servidores. Por otra parte, no se observa ningún cambio respecto de la información sobre los tratamientos y fines de los datos recabados.

155 RUIZ MIGUEL, CARLOS. *Protección de datos personales y comercio electrónico*… Pág. 409.

en los que tales operaciones se requieran para satisfacer la ejecución, cumplimiento o control de una relación jurídica entre afectado y responsable del fichero, según determinan los artículos 6 y 11 de la LOPD respectivamente. En este sentido, todas aquellas actuaciones que se realicen en red que encajen en los citados supuestos permiten captar, tratar y ceder cookies sin que intervenga la voluntad del afectado. Tales circunstancias concurren en los supuestos que implican una transacción, por regla general, no así en aquellos casos de mera consulta de una página o sitio. No obstante, existen muchos casos en los que la visualización de la página, sin más, exige la instalación de cookies, lo cual no resulta muy conforme con la legislación de protección de datos, pues se imposibilita el juego de la voluntad del afectado, que se ve compelido a dicha carga si desea conocer el contenido de la página.

Todos los planteamientos hasta ahora realizados tenían como finalidad determinar el grado de implicación que las cookies tienen con la protección de datos de carácter personal. No obstante, nuestro interés también radica en la posible configuración de las cookies como un supuesto de cesión de datos, no ya de recogida o tratamiento. A tales efectos, tenemos que volver a recordar algunos aspectos técnicos de estas herramientas.

Como ficheros de textos que se envían a los equipos clientes con el fin de almacenar información que posteriormente será remitida, las cookies son colocadas en dichos equipos por los servidores o proveedores de servicios. En principio, la información captada se remite después a dicho servidor. Podríamos, por tanto, concluir afirmando que se trata de un supuesto de recogida de datos, sin más. Sin embargo, esto no es del todo cierto, al menos no refleja la totalidad del proceso. Además de tal envío, la información de las cookies se envía a los sitios web que el usuario ha visitado, a los administradores de dichas páginas, con el fin de personalizar, matizar, etc., hacer más atractivo, en definitiva, el contenido de dicho sitio. Tal remisión no se produce en un momento posterior a la sesión de navegación, lo cual implicaría un supuesto de cesión tradicional, producida ésta fuera de los cauces propios de las telecomunicaciones. En este sentido, ninguna especialidad, desde el punto de vista normativo, se observaría. La cesión se hace de forma simultánea a la captación por el servidor del contenido de la cookie.

Sobre la base de lo expuesto anteriormente, podemos afirmar que las cookies presuponen una cesión o comunicación de datos de carácter personal. Los titulares de las páginas web *colgadas* de un servidor (término empleado para referirse a la circunstancia de que la página se alberga o se instala en un servidor) no tienen que coincidir necesariamente con los titulares de estos servidores. Por lo tanto, se trata de una revelación de datos a persona distinta del interesado y de quien los ha recogido inicialmente, lo cual coincide plenamente con la definición que de la cesión de datos se acoge en la legislación.

Resulta preocupante que la facilidad de la calificación efectuada no se corresponda con la aplicación que, en consecuencia, debería realizarse de la norma.

Como ya se ha dicho, el consentimiento genérico que el afectado pudiere prestar respecto de las cookies (el cual no concurre en nuestra opinión, como ya hemos señalado) en ningún puede hacerse extensivo a los fines posteriores a los que se destinen los datos, ante la falta de información al respecto. En menor medida se puede admitir dicha presunción como presupuesto para la admisión de estas cesiones. Quizás pudiere alegarse que la cesión que posibilitan las cookies es una consecuencia necesaria de la ejecución del contrato que une a los usuarios y a los servidores, para la prestación de los servicios de los segundos a los primeros. En tal caso, conforme se deduce del artículo 11.2 de la LOPD, se trataría de una circunstancia que eximiría de la necesidad de consentimiento para la cesión. Sin embargo, no se puede entender que toda la información que se recoge a través de las cookies resulta necesaria para la ejecución de las prestaciones propias de dicho contrato. Si dicha prestación consiste en la prestación de servicios, básicamente la oferta de páginas para que puedan ser visualizadas, entonces se podrán ceder sin tal consentimiento aquellos datos que sea necesarios para conseguir aquel objetivo, es decir, los datos necesarios para la navegación hasta dicha página. Por lo tanto, tal exención no puede beneficiar a los servidores respecto de la información que no sea pertinente a dichos efectos[156].

El Grupo de Trabajo[157] ha propuesto, como medida de fomento de la privacidad de los datos de los usuarios, la posibilidad de que los servidores puedan impedir el conocimiento de las direcciones IP a los sitios web, mediante la utilización de un *servidor proxy*[158]. En este caso, tal servidor haría las funciones de intermediario en la conexión con la página, de forma que la misma sólo sabría que la conexión procede de dicho servidor, pero no cuál es el equipo que desea conectar con la página a través del mismo. Una solución similar en los fines a la anterior consiste en la elección por los usuarios de sitios y programas que permiten ocultar la dirección IP mediante la utilización de servidores que sustituyen tal dirección[159].

---

[156] A tal efecto, debemos reseñar que la información susceptible de recogida por las cookies es muy variada y más extensa que la relativa a la mera navegación. Por ejemplo, es posible que las cookies puedan contener datos de identificación directa, como ya dijimos, que se hallan almacenados en el disco duro del ordenador. Pueden igualmente recoger los códigos de usuario y las contraseñas empleadas por éstos.

[157] *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*…Pág. 58.

[158] Se trata de un servidor que hace las veces de intermediario entre el usuario concreto que conecte a través del mismo y el resto de la red. Su principal beneficio consiste en que aporta gran velocidad de acceso a los contenidos de las páginas. En realidad, el contenido de las páginas se almacena en este servidor, de manera que los equipos conectados al mismo acceden al mismo sin que se descargue en éstos últimos. Por estas razones, muchas compañías utilizan este medio de conexión. No obstante, tenemos que decir que el mismo facilita el control de los sitios visitados desde los equipos de las compañías, lo que planteado problemas de protección de la privacidad de los empleados.

[159] También se han propuesto otras soluciones de carácter técnico. Por ejemplo, la segmentación física de los discos duros de los ordenadores. De esta forma, parte de la

No obstante reconocer los beneficios de estas medidas, sin embargo también se debe reconocer que, en la práctica, se trata de una solución poco utilizada: conseguir tal opacidad implica la asunción de gastos no exigidos por la normativa. Además, debemos tener en cuenta que los sitios que se alojan en un servidor desean contar con la información que éste les pueda proporcionar. Si un servidor adoptara tal medida con el fin de limitar dicha información, entonces vería disminuida la demanda de páginas instaladas en el mismo. En este sentido, se abriría una competencia en detrimento de quienes preservan los datos de los usuarios. Así, parece que la normalización normativa sería la solución más adecuada.

Dentro de las diferentes categorías y clasificaciones que existen de las cookies, nos interesa destacar, por su carácter especialmente pernicioso, la denominadas cookies activas. Concretamente nos referimos a los *applets de Java* y *los controles ActiveX*. Tales herramientas se instalan en el disco duro del ordenador del usuario y se dedican a comprobar los datos personales que pueden figurar en el mismo, pues se aprovechan de la información que se ha recogido por otras cookies[160].

---

información que se almacena en los ordenadores no sería accesible a las cookies, dado que las mismas se instalarían en una de esas partes del disco, impidiendo su acceso a las otras. Se trata de una operación que se utiliza con la finalidad de que cada parte generada por la segmentación se gestione con un sistema operativo diferente: por ejemplo, con Linux y con Windows. De esta forma, las cookies debería estar configuradas para poder recoger la información que se gestiona con ambos sistemas operativos. La mera partición lógica de los discos no sirve, en cuanto que en este caso es el mismo sistema operativo el que gestiona estas partes, de forma que las cookies podrían operar respecto de todas ellas.
El Consejo de Europa, en su Recomendación nº R (99) 5, de 23 de Febrero de 1999, propone a los proveedores de servicios una serie de medidas de protección de los datos de carácter personal. Junto al empleo de programas o servidores de anonimato, medios de seguridad y demás mencionados, también incluye las siguientes medidas: otorgamiento de pseudónimos a los internautas, información sobre los riesgos para la vida privada, consentimiento para la recogida y tratamiento de los datos. CONSEJO DE EUROPA. *Recomendación nº R(99)5 del Comité de Ministros de los Estados miembros sobre la protección de la Intimidad en Internet, para la protección de las personas respecto a la recogida y tratamiento de datos personales en las autopistas de la información.* Adoptada por el Comité de Ministros el 23 de febrero de 1999.

[160] Se trata de dos componentes, utilizados cada uno por los dos programas de navegación dominantes, respectivamente. Java es un lenguaje de programación creado por la empresa Sun Microsystems, que se utiliza en el navegador Navigator de Nestcape. En el caso de Active X, se trate controladores con fines de gestión multimedia, empleado por el Internet Explorer de Microsoft. Cada una de estas herramientas ha planteado problemas respecto de la confidencialidad de los datos de carácter personal que se relacionan con los citados navegadores. En el primer caso, un *script* permitía a un sitio web conocer la dirección de correo electrónico de un usuario. Ante la realidad de dicha posibilidad, Nestcape ha corregido tal anomalía en las versiones del Navigator posteriores a la 3.0. Respecto de Active X, varias voces se han alzado frente a Microsoft. Se ha demostrado que, mediante el uso de un componente de Active X, se podía acceder y destruir ficheros del ordenador del usuario, formatear su disco

Concretamente, tales controles permiten el conocimiento de: historial de navegación, identificación del usuario, direcciones de correo electrónico, agendas electrónicas y otras bases de datos[161].

Se trata de una categoría especial, pues en realidad la información contenida en las cookies no puede ser conocida de modo general: en realidad las cookies están asociadas a un sitio web y a un navegador en concreto, de manera que la información de una cookie creada por un servidor con ocasión de la visita de un sitio concreto, sólo puede conocida por el servidor que la ha enviado cuando el usuario vuelva a visitar el mismo sitio desde el mismo equipo y cuando utilice el mismo programa de navegación. En cualquier caso, las posibilidades ofrecidas por los dos tipos de cookies citados son mayores, lo cual es directamente proporcional a su potencial peligro. Las mismas implican, no ya una cesión acordada entre cedente y cesionario, sino una acceso indebido por cuanto que el primero, que recabó inicialmente la información, no ha tenido contacto alguno con quien pretende captar la información por estos medios. Todo ello, claro está, sin olvidar la ausencia del participación y control de los usuarios.

El alarmante vacío normativo existente respecto de las cookies ha sido cubierto por la Directiva 2002/58. Dispone su artículo 5.3 lo siguiente:

> *Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho a negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o por el abonado.*

Como se puede observar, el precepto exige la concurrencia de consentimiento previo e informado, circunstancias éstas que, como se ha tenido ocasión de comprobar, no se perciben en la práctica de los procesos de navegación. Aunque el precepto solamente exige el ofrecimiento de la posibilidad de negarse a la instalación de las cookies, sin embargo ello se traduce en la necesidad de

---

duro (lo que implica borrar toda la información) e incluso realizar operaciones utilizando el número de cuenta bancaria.

[161] RIBAS ALEJANDRO, JAVIER. *Riesgos legales de Internet. Especial referencia a la protección de datos personales.* En *Derecho de Internet. Contratación electrónica y firma digital.* Coord. MATEU DE ROS, RAFAEL y CENDOYA MENDEZ DE VIGO, JUAN MANUEL. Ed. Aranzadi. PAMPLONA, 2000. Pág. 157.

consentimiento previo, por la propia naturaleza de las cosas: la información previa se presta a través de la pantalla del equipo, acompañada de la opción aceptar o cancelar. Por lo tanto, se manifiesta o no consentimiento a la instalación[162].

A juicio de Cimas, la adopción de un sistema *opt-out*, es decir, de admitir la posibilidad al usuario de negarse, sin requerir una voluntad acorde, se debe a que el legislador comunitario quiso adoptar una posición intermedia entre la defensa de los usuarios de la red y los titulares de las páginas, para quienes las cookies prestan un servicio muy beneficioso, al facilitar el acceso a aquéllas[163]. En efecto, parece que con la solución apuntad se consigue una posición de satisfactoria, en parte, para los sujetos a quienes concierne el problema.

c. La identificación de la llamada entrante en la navegación por Internet.

Como ya vimos, se trata de una de las cuestiones por la que la protección de datos se ve afectada por las telecomunicaciones. Sin embargo, ya podemos adelantar que la solución adoptada respecto de las comunicaciones tradicionales, no se puede sostener respecto de la navegación por Internet. La configuración técnica de la red y de las conexiones efectuadas a través de la misma impide tales concepciones.

En el proceso de navegación, los equipos clientes solicitan a los servidores que les remitan una información concreta, la que se acoge en una página determinada, para lo que habrá que comunicarle cuál es la dirección IP del

---

162 A pesar de su extensión, a continuación incluimos en estas líneas el Considerando 25 de la Directiva 2002/58, pues el mismo recoge de forma clara los diversos problemas y posibles soluciones que hemos expuesto, referentes a las cookies. Se afirma en aquél: *No obstante, los dispositivos de este tipo, por ejemplo los denominados «chivatos» (cookies), pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo, para analizar la efectividad del diseño y de la publicidad de un sitio web y para verificar la identidad de usuarios partícipes en una transacción en línea. En los casos en que estos dispositivos, por ejemplo los denominados «chivatos» (cookies), tengan un propósito legítimo, como el de facilitar el suministro de servicios de la sociedad de la información, debe autorizarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un «chivato» (cookie) o dispositivo semejante. Esto es particularmente importante cuando otros usuarios distintos al usuario original tienen acceso al equipo terminal y, a través de éste, a cualquier dato sensible de carácter privado almacenado en dicho equipo. La información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores. La presentación de la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante, se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un «chivato» (cookie) o dispositivo similar, en caso de que éste tenga un propósito legítimo.*

163 CIMAS, MARTA. *Protección de datos y telecomunicaciones. Regulación actual y exigencias de la nueva Directiva.* En *la nueva regulación de las telecomunicaciones, la televisión e Internet.* VILLAR URIBARRI, JOSE MANUEL (Director). Ed. Thomson-Aranzadi. MADRID, 2003. Pág. 302-3.

destinatario. Una vez que el servidor ha localizado, por la dirección aportada, cuál es la página que se desea consultar, se comunica con el equipo cliente para remitirle la información solicitada. Claro está, para poder remitirle la misma, es necesario que el servidor conozca cuál es la dirección IP, dinámica o estática, como hemos visto, del equipo cliente. Es decir, es imposible acceder a una página web sin dar a conocer la dirección del equipo desde el que pretendemos conectar con la misma.

Tal necesidad es consecuencia de la estructura de las conexiones en la red. En una llamada telefónica tradicional, los equipos conectados entre sí ocupan de forma continua un cauce de comunicación, una línea. Es decir, mientras dura la conversación se mantiene ocupada tal línea, sin que en ningún momento se corte dicha comunicación. Por esta razón, si tratamos de comunicar con alguien que está hablando a través de ese teléfono, no podremos hacerlo porque *comunica*. Se trata de una comunicación continua. En cambio, en Internet la comunicación se efectúa mediante las llamadas *conexiones sin estado*. Tal terminología hace referencia a la circunstancia de que tales conexiones son intermitentes, de forma que remitida la información solicitada por parte del servidor al cliente, la conexión se cierra. Si el último solicita más información, entonces se abre de nuevo la comunicación con el servidor, lo cual requiere de nuevo la identificación del solicitante. Tal forma de comunicación de justifica por la agilidad y rapidez que se consigue, dado que la multitud de líneas permanecen cerradas lo necesario, evitando la sobrecarga de las mismas. La imposibilidad de mantener una línea exclusiva impide el conocimiento previo de quien desea conectar con el servidor. Técnicamente, la identificación del equipo se consigue porque en la cabecera del paquete de información que se transmite al servidor, va inserta la dirección IP.

Así, la regulación sobre identificación de línea entrante y conectada no es de aplicación a las conexiones efectuadas por Internet. Como ha señalado el Grupo de Trabajo[164], el artículo 8 de la Directiva 97/66 no era aplicable a las direcciones IP. Por la misma razón, apunta aquél que la Propuesta de Directiva acertaba al mantener el término *llamada*, desechando el de *comunicación* en el precepto relativo a esta cuestión, lo que supone su mantenimiento para las comunicaciones telefónicas tradicionales de forma exclusiva. En efecto, es esta la solución adoptada finalmente en la Directiva 2002/58, cuyo artículo 8.1 dispone que

> *1. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor de servicio deberá ofrecer al usuario que efectúe la llamada la posibilidad de impedir en cada llamada, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen. El abonado que origine la llamada deberá tener esta posibilidad para cada línea.*

---

[164] *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*…Pág. 57.

No obstante, no debemos olvidar que en una conexión a Internet se está realizando una llamada telefónica, de modo que también se generan datos de tráfico propios de éstas. En tal caso, el tratamiento de la identificación del número telefónico desde el que se efectúa la llamada no puede ser el mismo que el proporcionado a la dirección IP asignada a la sesión de conexión. En efecto, el primero se encuentra inmerso dentro de los datos de tráfico y facturación que el operador de telecomunicaciones que facilita la comunicación con el proveedor de acceso puede conocer por las razones y los fines ya apuntados en el epígrafe anterior. Ahora bien, la identificación de la llamada entrante, en el caso de la navegación por Internet y respecto de los citados datos de tráfico exclusivamente telefónicos, se plantea precisamente con relación al proveedor de acceso. Parece que en este caso tal cuestión debe resolverse a la luz de la regulación sobre identificación de la llamada entrante, la cual permite la misma, según vimos, con las limitaciones ya descritas. El proveedor de servicios no tendrá acceso a tal información, pues no es el mismo quien recibe directamente la llamada. No obstante, la obtención de la dirección IP resulta suficiente para satisfacer sus objetivos.

A salvo lo anterior, la exclusión de la regulación del artículo 8 de la Directiva respecto de los actos de navegación por Internet, se refuerza si tenemos en cuenta que la Directiva 2002/58 incluye une definición de llamada separada de la de comunicación electrónica, ya vista. El artículo 2 e) define aquélla como

> *Una conexión establecida por medio de un servicio telefónico disponible para el público que permita la comunicación bidireccional en tiempo real.*

Aunque el uso de un servicio telefónico no es exclusivo de este tipo de comunicación, sin embargo el carácter bidireccional en tiempo real permite distinguir las llamadas de las comunicaciones electrónicas.

> d. Las cesiones o comunicaciones de datos realizadas como consecuencia de las fusiones y escisiones de empresas. Las cesiones de datos en los grupos de empresas.

Aunque se trata de una posibilidad que se plantea respecto de todo tipo de empresas responsables de ficheros de datos personales, sin embargo el novedoso y vertiginoso desarrollo de *las empresas .com*, junto con la crisis financiera que gran parte de estas empresas han experimentado en los últimos tiempos, ante el incumplimiento de unas desmesuradas expectativas iniciales, ha ocasionado que estas operaciones hayan proliferado dentro de este sector[165]. A este respecto, se ha defendido dos

[165] Uno de los casos de fusión de empresas que prestaban servicios de Internet fue la fusión de Double Click, empresa de servicios publicitarios y de marketing en Internet, con Abacus Direct Corporation, la cual explotaba ficheros de datos de carácter personal con los mismos fines. Doubleclick anunció que cruzaría los ficheros de ambas entidades (fue una fusión por absorción de la primera sobre la segunda), lo cual provocó reacciones de los usuarios, que llegaron hasta los tribunales.

posiciones: por una parte, se sostiene que, como supuesto de traspaso a otro sujeto, implica una cesión o comunicación de datos, que determinaría la aplicación del régimen jurídico propio de las mismas. Por otra, se entiende que se trata de una operación que, si bien conlleva el citado traspaso, sin embargo no puede considerarse tal cesión o, en su caso, no será de aplicación el régimen de las cesiones[166].

Las operaciones de fusión y escisión de sociedades dan lugar a la aparición de personas jurídicas diferentes de las anteriores, que en nuestro caso se configuran como responsables de los ficheros de las anteriores. En el borrador del Proyecto de la LOPD se establecía, a este respecto, lo siguiente:

> *Cuando se produzca un cambio en la responsabilidad del tratamiento, ya sea por su transmisión a un tercero, ya por la absorción, fusión o segregación empresarial, el nuevo responsable deberá notificar su identidad a los interesados, informándoles de los derechos de acceso, rectificación y cancelación y del lugar en que puedan ejercerse.*
>
> *El cambio en la responsabilidad del tratamiento no se considerará comunicación de datos.*

Parece que la intención inicial del legislador era la de eximir a las compañías de la farragosa tarea de la solicitud del consentimiento para la cesión de los datos a la compañía resultante. No se puede negar que el volumen de operaciones que implica tales estrategias empresariales se dificulta aún más con la necesidad de satisfacer los requisitos que, de modo general, exige la legislación sobre protección de datos.

Otro fenómeno similar, que puede afectar al régimen de las cesiones de datos de carácter personal, es la existencia de grupos de empresas. Respecto de esta figura, muy utilizada en el ámbito empresarial actualmente por motivos financieros y de control de las actividades, parece claro que la cesión o comunicación de datos entre las mismas responde al modelo genérico de cesión, de manera que las mismas se deben ser sometidas a los mismos requisitos que cualquier otra cesión, pues se trata de entidades diferentes con personalidad jurídica propia. No obstante, tal circunstancia se tiene en cuenta hoy día por las compañías, las cuales incluyen en el formulario de solicitud de datos una cláusula por la que se entiende concedido el consentimiento para las cesiones entre empresas del grupo. Sobre este punto, APARICIO SALOM, JAVIER. *Estudio sobre la Ley Orgánica de Protección de datos de carácter personal.* Págs. 34 y 35.

[166] Esta cuestión ha sido objeto de análisis, por nuestra parte, en el artículo *Cesión de datos, fusión y escisión de sociedades. Los grupos de empresas.* Revista datospersonales.org (revista digital de la Agencia de Protección de Datos de la Comunidad de Madrid). Nº 4, de 16 de Septiembre de 2003. Pág. 2

En este sentido, Miralles Miravet y Baches Opi[167] sostienen que las cesiones que se ocasionan como consecuencia de estos procesos de concentración o disgregación pudieran haberse exceptuado de los requisitos del artículo 11 a la luz de la Directiva 95/46/CE. Concretamente, el artículo 7 f) de la misma evita la necesidad de consentimiento para la cesión cuando la misma se requiera para satisfacer un interés legítimo del responsable del tratamiento o de los cesionarios, siempre, claro está, que no prevalezcan los derechos fundamentales de los afectados. A este respecto, señala Heredero Higueras que este precepto comunitario acoge el concepto de interés prevalente, propio de la legislación alemana de 1990[168]. Según este autor, el artículo 7 f) acoge los intereses de mercado, la competencia leal y la libre circulación de datos en el seno del mercado interior, a que se refiere la Directiva en otros pasajes. Ahora bien, como afirma Heredero, la norma comunitaria no determina específicamente cuáles son esos intereses prevalentes, es decir, los supuestos concretos en los que entra en juego esta regla, sino que tal decisión es competencia de los Estados miembros[169]. En este sentido, parece que hubiera sido necesaria una previsión legislativa al respecto.

En relación con lo anterior, debemos tener en cuenta que con esta exclusión del concepto de cesión se satisfaría un interés de naturaleza particular, frente a los intereses públicos o generales a que responden las excepciones contenidas en el artículo 11.2 de la LOPD. Es decir, la normativa parece identificar los intereses legítimos a que se refiere la Directiva con todos aquéllos que persigan un fin de carácter general. A lo anterior, debemos añadir que la necesidad del consentimiento del afectado en estos casos no supone una vulneración de la libertad de empresa del artículo 38 de la Constitución, a diferencia de lo que, en caso contrario, se observa respecto del derecho a la Autodeterminación informativa. Sea como fuere, lo cierto es que la voluntad definitiva del legislador, a la luz del texto de la LOPD, ha sido la contraria. El silencio a este respecto de la Ley, cuando en el *iter* parlamentario de la LOPD se había pretendido introducir sin éxito una excepción en el sentido mencionado, permitiría afirmar que tales casos conllevan cesiones de datos de carácter personal, las cuales se regirán por el régimen general que la misma contiene, como de hecho se puede observar en la práctica[170].

---

[167] MIRALLES MIRAVET, SERGIO y BACHES OPI, SERGIO. *La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos*. Revista de Derecho de Derecho Privado. Mayo de 2001. Págs. 438-439.

[168] HEREDERO HIGUERAS, MANUEL. *La Directiva comunitaria de protección de datos de carácter personal*. Ed. Aranzadi. PAMPLONA, 1997. Pág. 112.

[169] HEREDERO HIGUERAS, MANUEL. *Op. cit*. Pág. 112.

[170] Esta solución es la que fue adoptada en el proceso de absorción de la empresa Wanadoo, empresa de servicios de Internet perteneciente en su mayoría a France Telecom. En una carta dirigida a los abonados, se comunicaba que la falta de comunicación en contrario suponía la aceptación de la cesión de los ficheros a la empresa resultante. La citada misiva debía estar completada con las informaciones que exige el artículo 5.4 de la LOPD (procedencia de los datos, existencia del fichero, finalidad del tratamiento y destinatarios; ejercicio de los derechos

No obstante y como vamos a observar a continuación, la posición adoptada respecto de los procesos de fusión no es, con mucho, pacífica. Por el contrario, son muchas las voces (entre ellas, la propia Agencia Española de Protección de Datos) que sostienen la opinión contraria, negando que tales supuestos sean constitutivos de una cesión o comunicación de datos. Para ello, se recuerda la configuración de las fusiones de sociedades como un caso de sucesión universal. En efecto, establece el artículo 233.1 de la LSA que

> *La fusión de cualesquiera sociedades en una sociedad anónima nueva implicaría la extinción de cada una de ellas y la transmisión en bloque de los respectivos patrimonios sociales a la nueva entidad que haya de adquirir por sucesión universal los derechos y obligaciones de aquellas.*

Tal consideración elimina la posibilidad de aplicar, en tales casos, el artículo 1205 del Código Civil, que concluiría en la necesidad de que concurra el consentimiento de los acreedores para el traspaso de las distintas relaciones que se pretenden transmitir, lo que mermaría los beneficios de los procesos de fusión[171]. A lo anterior, se debe afirma por algunos que los traspasos en bloque que se producen con motivo de la sucesión universal, no sólo tienen por objeto elementos de naturaleza puramente patrimonial, sino que pueden afectar a relaciones de carácter personal, de forma análoga a lo que se afirma respecto del contenido de la sucesión *mortis causa*[172]. No obstante, en la mayoría de estos supuestos, se observa, más bien, el traspaso de una relación patrimonial que ocasiona, a su vez, efectos en la esfera personal.

La tesis favorable a la exoneración del consentimiento del afectado en las cesiones de datos provocadas por los procesos de fusión encuentra su mayor apoyo en la concepción amplia de la sucesión universal, como ya hemos dicho anteriormente, y en la propia LOPD. En efecto, si bien el artículo 11.2 c) no acoge todos los supuestos de cesiones por fusión, sin embargo sí lo hace el apartado a) del mismo precepto. Según el mismo, no se requiere consentimiento alguno del afectado cuando la cesión esté amparada por una Ley. Pues bien, sobre la base de la inclusión de las relaciones personales en la sucesión universal y de que la misma se contempla expresamente en la LSA, estas cesiones no requerirían consentimiento alguno. Esto, a su vez, explicaría

---

de acceso, rectificación, cancelación y oposición y, finalmente, identidad y dirección del responsable del fichero y de su representante), como recuerdan Miralles Miravet y Baches Opi. MIRALLES MIRAVET, SERGIO y BACHES OPI, SERGIO. *Op. cit.* Pág. 438.

171 URIA, RODRIGO. *Derecho Mercantil.* Ed. Marcial Pons. MADRID, 1998. Pág. 395.

172 No obstante, esta posición no es, con mucho, unánime. Uría alude únicamente a transmisión de patrimonios. URIA, RODRIGO. *Op. cit.* Págs. 395-396. En el mismo sentido se pronuncia Sánchez Calero. SANCHEZ CALERO, FERNANDO. *Instituciones de Derecho Mercantil. Vol. I.* Ed. MCGraw Hill. Madrid, 2000. Pág. 551.

porque el texto final de la LOPD no incluyó precepto alguno respecto de estas cuestiones.

Es conveniente recordar que los datos de carácter personal son objeto de un derecho de la personalidad que, sin negar la posibilidad de su consideración o significación económica, no por ello se puede abdicar de las características de un derecho de tal naturaleza. En este sentido, las bases de clientes de una sociedad forman parte del activo de la misma, sin embargo ello no conlleva su consideración exclusiva como un elemento patrimonial de la misma. Es decir, no es posible adoptar una decisión que únicamente tenga en cuenta intereses de naturaleza puramente patrimonial.

No es discutible, en ningún caso, la concepción de las fusiones como un caso de sucesión universal: lo contrario sería negar la propia norma. Ahora bien, tal afirmación no implica, en nuestra opinión, aceptar sin más la exclusión de las cesiones en las fusiones. La sucesión universal implica el traspaso en bloque del conjunto de relaciones, activas y pasivas, del o los sujetos fusionados a otro sujeto, ya sean de nueva creación o previamente existentes. Así, no se produce el efecto extintivo-constitutivo de aquéllas, a la vez que se eliminan los inconvenientes que se derivarían de la realización de una serie de actos de transmisión, diversos en función del tipo y naturaleza de la relación de que se trate: en la fusión no hay liquidación[173]. Sin embargo, es igualmente innegable que todo ello se produce conjuntamente con la desaparición de un sujeto y la aparición de otro diferente. Según el artículo 233.1 de la LSA,

> *La fusión de cualesquiera sociedades en una sociedad anónima nueva implicaría la extinción de cada una de ellas…*

Es decir, la sucesión universal, si bien permite la permanencia inmodificada de la mayoría de los elementos de una situación jurídica, sin embargo supone la alteración de uno de los elementos subjetivos de la misma. Es más, si no existiese dicha alteración, entonces no se justificaría la existencia de tal construcción, pues si nada cambia, no es necesario adoptar soluciones que permitan la mínima modificación. En palabras de Garrigues, "sin disolución no hay fusión"[174].

Sobre la base de todo lo anterior, debemos recordar que el dato decisivo de una cesión o comunicación de datos no es la conservación de la relación existente entre afectado y responsable del tratamiento en la mayoría de sus elementos, sino precisamente la aparición de un nuevo sujeto, sin distinguir si dicha aparición constituye una nueva relación o por el contrario se produce mediante la conservación

---

[173] Entre otros, se puede citar GARRIGUES DIAZ-CAÑABATE, JOAQUIN. *Tratado de derecho mercantil. Tomo I, vol. 3º*. Revista de derecho mercantil. MADRID, 1947-1964. Pág. 1273-4.

[174] GARRIGUES DIAZ-CAÑABATE, JOAQUIN. *Op. cit.* Pág. 1271.

de la ya existente. Recordemos que se considera cesión toda revelación de datos a persona distinta de su titular. Nada más se exige en el artículo 3 de la LOPD. Es decir, a la norma no le preocupa si se produce un efecto transmisivo o, por el contrario, continuista de la situación anterior: únicamente la alteración de los sujetos. El concepto de cesión que deduce de la LOPD no exige un acto de transmisión de la información, sino que es más bien, consecuencia de la naturaleza del propio bien que se "traspasa", un acto de comunicación, de puesta en común de la información. Así, podría pensarse que la institución de la sucesión universal, creada para evitar los inconvenientes de las transmisiones individuales de un conjunto de relaciones, no tiene justificación en estos casos, en los que no se produce efecto extintivo alguno, puesto que la información no se pierde para el cedente. Por tanto, el dato decisivo de la cesión o comunicación de datos de carácter personal es la aparición de un nuevo sujeto, no el mantenimiento o no de las relaciones existentes.

Los supuestos de comunicación de datos como consecuencia de las fusiones de sociedades, pudieran acaso subsumirse en el supuesto de hecho del artículo 11.2 c) de la LOPD. Según este precepto, no es necesario el consentimiento del afectado cuando el mismo sea parte en una relación contractual, entre otras, para cuyo mantenimiento, control y ejecución sea necesaria la comunicación de los datos personales. No obstante, tal precepto tan sólo sería aplicable en aquellos casos en los que todavía existiera una relación pendiente de cumplimiento, es decir, aquellos que constituyen un supuesto de cesión de contrato. Tal exigencia excluiría esta solución respecto de aquellos supuestos en los que los datos de carácter personal obran en poder del responsable como consecuencia de una relación ya concluida, como ocurre en la mayoría de los casos.

Respecto de los diversos procesos anteriormente mencionados, es también doctrina relativamente común aquélla que sostiene que, en realidad, en todos ellos se observa un supuesto de subrogación. De esta forma, se entiende que las entidades resultantes no ocupan su posición en una relación nueva con los afectados, sino que tan sólo se ha producido una modificación subjetiva de la misma. En tal sentido, no existe cesión de datos, puesto que no se observa el efecto extintivo y creador de una transmisión: se mantiene la misma situación jurídica. Sin perjuicio de reconocer que, en efecto, se observa un supuesto de sucesión en las relaciones jurídicas de las entidades originales, ello no quiere decir, a mi modo de ver, que necesariamente no nos encontremos ante un supuesto de cesión o, dicho de forma más correcta, de comunicación.

La subrogación es una institución jurídica en virtud de la cual se mantiene la relación jurídica en los supuestos de sustitución o alteración subjetiva. Concretamente, por la subrogación perdura la relación existente tras el cambio de acreedor. Así, se entiende que el mantenimiento de la misma relación, siquiera modificada, impide la calificación del supuesto como cesión o comunicación de datos, lo que elimina la necesidad de que concurra el consentimiento.

No obstante lo anterior, no se debe olvidar que el dato decisivo para calificar un acto como cesión o comunicación es la aparición de un nuevo sujeto responsable del tratamiento de los datos. El concepto de comunicación de datos de carácter personal que acoge el artículo 3 de la LOPD no alude a la necesidad o no de mantener la misma relación, sino únicamente al cambio de sujeto (cesión como transmisión efectiva) o a su acumulación al anterior (comunicación de datos). Es decir, existe cesión o comunicación cuando los datos se revelan a otro sujeto. A tal efecto, poco importaría el mantenimiento o la extinción de la relación. Es más, en la mayoría de los casos de comunicaciones de datos el responsable de los datos inicial no "desaparece", sino que el nuevo accede a los datos que aquél continúa conservando. Tal situación se asimilaría, más bien, a una asunción cumulativa de las obligaciones, situación que no concurre, generalmente, en estos procesos de concentración o escisión.

En realidad, la solución a este problema debe encontrarse en los propios conceptos de cesión o comunicación, por una parte, y de sucesión universal, por otra. En el primer caso, debemos reseñar que el concepto de cesión hace alusión, no tanto a la transmisión efectiva de la información, sino, por la propia naturaleza de ésta, a la puesta en común de la misma por parte de su tenedor. De esta forma, se incluyen muchos supuestos que, sin llegar a concluir una transmisión efectiva, sin embargo implican revelación. Así, lo que se pretende evitar, en última instancia, en la desmesurada ampliación del círculo de conocedores de los datos de carácter personal.

En la sucesión universal producida por las fusiones de sociedades, la desaparición de uno de los sujetos, el fusionado, impide hablar de ampliación del citado círculo. Como cualquier supuesto de sucesión, se trata de la sustitución de un sujeto por otro, el cual se despoja totalmente de los datos, en cuanto deja de existir. Así, aunque en sentido estricto existe revelación de datos a un sujeto distinto, sin embargo no se puede hablar de puesta en común, dado que el supuesto cedente deja de poseer la información. Por lo tanto, el sentido del concepto de cesiones o comunicación de datos que recoge el artículo 3 de la LOPD no parece coincidir con el de los casos de sucesión universal.

La solución aportada respecto de los procesos de fusión de sociedades, es predicable de todos ellos, tanto los que constituyen la fusión propia, con creación de una entidad diferente de las fusionadas, como de los casos de fusión impropia o por absorción, en los que se mantiene la personalidad jurídica de sociedad absorvente. En uno y otro caso se observa la misma realidad: falta el dato de la dispersión de la información, dado que el resultado final la sociedad "cedente" forma parte, al desaparecer, de la estructura de la sociedad nueva o de la absorvente. Por lo tanto, es aplicable lo dicho hasta ahora con carácter general. Todo ello, sin desconocer que el artículo 233.2 de la LSA configura también este supuesto como otro caso de sucesión universal.

En el supuesto de procesos de escisión de compañías societarias por extinción de la original y creación de otras diferentes, es claro el resultado de generación o aparición de nuevas personas jurídicas, de lo que se deduce la transmisión de los datos de carácter personal a un nuevo sujeto y, por tanto, la existencia de un acto de comunicación o cesión de los mismos. En el caso de segregación de una parte, la solución sería idéntica respecto de los datos transmitidos a la segregada. Algún autor sostiene que, en los supuestos de escisión, nos encontramos ante un caso de duplicación del tratamiento de los datos de carácter personal[175].

Efectivamente, la escisión, como operación de desdoblamiento de la unidad inicial, supone necesariamente la utilización simultánea de los datos obrantes en los ficheros por las dos o varias sociedades resultantes de este proceso. Sin embargo, el empleo del término duplicación no impide mantener, también en este supuesto, su calificación como cesión o comunicación de datos. Es más, se corresponde perfectamente con el significado atribuido al término comunicación, del que se deduce, como se estudia en el primer capítulo de este trabajo, la puesta en común de información, no tanto la dualidad *pérdida-adquisición* propia de los procesos transmisión efectiva. Así, no plantea problema alguno la calificación de los supuestos de traspaso de datos de carácter personal a consecuencia de los procesos de escisión, como supuestos de cesión o comunicación de datos. En consonancia con el argumento central sostenido en líneas anteriores, sí se puede afirmar que los casos de segregación societaria constituyen, respecto de los datos de carácter personal, un supuesto de cesión o comunicación de datos.

Actualmente, existe otro problema diferente al derivado de los procesos de concentración o segregación y que también plantea problemas respecto del concepto de las cesiones de datos. En la actualidad, la evolución económica ha provocado la aparición de grandes grupos empresariales resultantes de procesos de concentración. Tales grupos pueden, por una parte, encuadrar diversas entidades que participan en un sector económico más o menos amplio (por ejemplo, los grupos de telecomunicaciones). Por otra, existen conglomerados (como los *chaebol* coreanos, que fabrican microondas, buques petroleros o coches). En el ámbito de Internet, muchas de estas empresas están integradas en estas estructuras.

La Agencia Española de Protección de Datos ha manifestado su preocupación al respecto[176]. En efecto, aunque en la mayoría de los casos la recogida de datos va acompañada de una cláusula relativa a estas cesiones, sin embargo la gran variedad de actividades desarrolladas por estos grupos pudiere ocasionar que las mismas no fueren del todo acordes con la voluntad inicial del afectado, que desconoce en su totalidad el destino de los datos. Por otra parte, entendemos que, en muchos

---

[175] APARICIO SALOM, JAVIER. *Estudio sobre la Ley Orgánica*… Pág. 182.

[176] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 2000*. Págs. 195-196.

casos, estas comunicaciones o cesiones pueden vulnerar el principio de finalidad de los datos del artículo 4 de la LOPD, cuando las especificaciones recogidas en el clausulado no hagan referencia expresa al respecto.

En cualquier caso, no se puede dudar de la existencia de un supuesto de cesión o comunicación en todos estos traspasos de información entre sociedades del mismo grupo. Así lo pone de manifiesto la Agencia de protección de datos[177], la cual coincide, según ella misma señala, con el parecer de los pronunciamientos judiciales existentes hasta el momento sobre esta cuestión. En efecto, en la sentencia de 16 de Octubre de 2000, del Tribunal Superior de Justicia de Madrid, se puede leer lo siguiente:

> *…cualquier empresa es libre de constituirse en cualquiera de las formas societarias que el Derecho mercantil regula. Asimismo, las empresas que pueden unirse a través de las distintas formas reguladas en derecho: fusión, absorción, sociedades anónimas y, como tales, independientes y con personalidad jurídica autónoma y que por el hecho de que la una sea propiedad de la otra, el particular que contrata con la primera pueda verse perjudicado, precisamente, por la estructura empresarial que la sociedad ha elegido. Si la recurrente ha preferido constituir dos sociedades y trabajar con ellas de manera independiente, beneficiándose así del mantenimiento de dos personas jurídicas distintas, no puede, al mismo tiempo, pretender justificar el conocimiento por parte de la matriz de los datos que le constan a la filial por las operaciones en que ésta última ha intervenido, pues ello supone olvidarse de que se trata de personas jurídicas distintas. Por otro lado, si el particular contrata con la filial, es a esta sociedad a la que, voluntariamente, se le comunican los datos que, en consecuencia, la filial no puede comunicar a la sociedad matriz en perjuicio del particular…*

Se deduce claramente que la existencia de personas jurídicas diferentes, siquiera integradas en un grupo empresarial, es dato suficiente para considerar la transmisión de la información, en estos casos, como un supuesto de cesión o comunicación de datos. A su vez, la prestación del consentimiento para el tratamiento de los datos por una compañía de tales grupos no faculta para realizar cesiones, sino que exige la concurrencia de un consentimiento específico para tales operaciones. De ahí que, en la práctica, las compañías incluyen cláusulas en los formularios de solicitud de datos relativas a estos actos.

Igualmente, del texto reproducido en líneas anteriores se deduce la misma solución respecto de los casos de transmisión de información como consecuencia de procesos de fusión de sociedades. Aunque no es el caso que se resuelve con ocasión de esta sentencia, podría entenderse que el Tribunal coincide,

---

177 AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 2000*. Pág. 431.

siquiera indirectamente, con las opiniones manifestadas anteriormente, relativas al rechazo de las argumentaciones derivadas de la consideración de las fusiones como un supuesto de sucesión universal.

Diferente del supuesto anteriormente analizado es el relativo a las transmisiones de datos de carácter personal entre personas que forman parte de una misma organización o entidad. Aunque pueda guardar relación con las cuestiones que se estudian en estas líneas, sin embargo consideramos más adecuado un tratamiento más detenido, que no corresponde realizar en estas líneas, pues este problema está en íntima conexión con la determinación de los sujetos que intervienen en la cesión.

4. El comercio electrónico.

Uno de las funciones de Internet que más se está desarrollando en los últimos años es el comercio electrónico. La definición de este concepto se ha realizado de forma amplia, evitando que se remita estrictamente a las adquisiciones de bienes y servicios. Así, se incluyen dentro del mismo cuestiones relativas a publicidad, información sobre bienes o servicios, atención al cliente, etc., con independencia de que se trate de actos remunerados ni que el pago se efectúe por el usuario o por terceros, según ha determinado el TEDH en su jurisprudencia y se deduce directamente de la letra a) del Anexo de la LSSICE. En realidad, se trata de equiparar los conceptos de comercio electrónico y servicios de la sociedad de la información.

Aunque desde un punto de vista técnico no sea muy correcto realizar dicha asimilación[178], sin embargo tiene interés para manifestar el carácter poliédrico del mismo, en cuanto afecta a muy diferentes cuestiones y se puede analizar desde diversas ópticas. De todas formas, el concepto legal de comercio electrónico no es restringido, dado que hace hincapié en el intercambio de información por las redes y no sólo de bienes y servicios, según se deducía del Artículo 2 a) del Anteproyecto de Ley sobre servicios de la Sociedad de la información:

> *toda forma de transacción o intercambio de información comercial basada en las transmisión de datos por redes de telecomunicaciones como Internet.*

Según manifiesta Aced Félez, esta definición incluye tanto las estrictas transacciones de bienes y servicios como aquéllas en las que los objetivos perseguidos trascienden al mero intercambio económico: mejora en la calidad, servicios que sólo se

---

[178] De modo similar a la Directiva 98/34, el Anteproyecto de Ley de servicios de la Sociedad de la información afirmaba, en su Exposición de Motivos, que entre aquéllos se encuentran los actos de comercio electrónico. De forma expresa lo establece el artículo 2 b) de la LSSICE, según el cual son *servicios de la sociedad de la información o servicio: además del comercio electrónico, todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.*

pueden prestar por red, entre otros[179]. Por lo tanto, respecto de la actividad de intercambio de información, resulta obvio que la misma puede ser de naturaleza personal.

De lo anterior, podemos deducir que todos aquellos supuestos en los que, no observándose la actividad comercial en sentido propio, sin embargo subyace un claro interés al respecto, se puede definir como operaciones de comercio electrónico. No obstante, diversos autores prefieren restringir el concepto, para referirse exclusivamente a las operaciones de naturaleza comercial[180].

En relación con lo dicho anteriormente, la LSSICE define, de forma más concreta, el contrato electrónico en la letra h) de su Anexo, como

> *Todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones[181].*

Es decir, se puede afirmar que el concepto de comercio electrónico es más amplio que el de contratos electrónicos, referido aquél a los servicios que, de modo más o menos general, poseen un objetivo comercial, y éste a las operaciones de carácter puramente contractual. Además, la redacción empleada en la definición del contrato electrónico nos induce a estar de acuerdo con Vattier Fuenzalida[182], para quien de aquélla se deduce que el legislador no ha pretendido crear una categoría contractual autónoma de las ya existentes, sino que tan sólo se reseña la especialidad derivada del medio o vehículo empleado y, por ello, las especificidades que la regulación debe contemplar al respecto.

---

179 ACED FELEZ, EMILIO. *Transacciones electrónicas en Internet.* Jornadas sobre Protección de la Privacidad, Telecomunicaciones e Internet. Pamplona, 2000. Pág. 2.

180 BOTANA GARCIA, GEMA ALEJANDRA. *Noción de comercio electrónico.* En *Comercio electrónico y protección de los consumidores.* Coord. BOTANA GARCIA, GEMA ALEJANDRA. Ed. La Ley. MADRID, 2001. Pág. 57. También MARTINEZ NADAL, APOLONIA. *La protección del consumidor en la Propuesta de Directiva sobre determinados aspectos del comercio electrónico.* Cuadernos de derecho y comercio, núm. 29. 1999. Pág. 114.

181 Algunas autores habían sostenido que, en realidad, el vehículo de transmisión de la oferta no tenía que ser necesariamente electrónico, siempre que la aceptación hubiese sido trasmisitida por este medio, pues es la conjunción de voluntades la que se debe producir en la red. En este sentido, RAYNOUARD, ARNAUD. *La formation du contract électronique.* En *Le contract électronique.* Travaux de l´Association Henri Capitant. Journées nationales, Tomo V. Toulouse, 2000. Ed. Panteón-Assas. PARIS, 2002. Pág. 20.

182 VATTIER FUENZALIDA, CARLOS. *Responsabilidad contractual y extracontactual en el comercio electrónico.* En *Régimen jurídico de Internet.* CREMADES, JAVIER; FERNANDEZ-ORDOÑEZ, MIGUEL ANGEL; ILLESCAS, RAFAEL (Coordinadores). Ed. La Ley. MADRID, 2002. Pág. 1186.

En línea con lo señalado anteriormente, la expresión contrato electrónico hace referencia al modo de celebración en sentido amplio de un contrato (preparación, celebración, ejecución y obligaciones posteriores), en el que se emplean mecanismos y lenguaje informáticos y electrónicos[183]. En cualquier caso, es cierto que estos términos se utilizan como complementarios, pues los mismos aluden a realidades unidas de forma indisoluble: el acto que se realiza y el medio a través del cual se lleva a cabo. De ahí que, en muchas ocasiones, se dote al término comercio electrónico de un significado extenso: transacción que se realiza mediante en empleo de redes de telecomunicaciones, como afirma Márquez Lobillo[184].

Por supuesto, nadie puede discutir que en la celebración de estos actos de comercio, que, en la mayoría de los casos, implican la celebración de un contrato, resulta imprescindible la identificación de las partes, concretamente la de los adquirentes, los consumidores. Sin embargo, ello no otorga facultades ilimitadas a los comerciantes respecto de estos datos, sino que obliga a que en las operaciones de comercio electrónico se tenga en cuenta el régimen jurídico y las limitaciones propias del tratamiento de los datos de carácter personal.

La Directiva 2000/31, sobre comercio electrónico, establece en su artículo 1.5 b) (ámbito de aplicación) que

La presente Directiva no se aplicará:

b) a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE (Esta referencia debe entenderse realizada a la Directiva 2002/58, según determina su artículo 19).

En relación con lo anterior, se afirma en el Considerando 14 de la Directiva lo siguiente:

La protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE de Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Directiva 97/66/CE del

---

183 MADRID PARRA, AGUSTIN. *Contratación electrónica.* En *Estudios jurídicos en homenaje al Profesor Aurelio Menéndez.* Tomo III. Ed. Civitas. MADRID, 1996. Pág. 2940. También, MARQUEZ LOBILLO, PATRICIA. *Empresarios y profesionales en la sociedad de la información.* Cuadernos Mercantiles. FERANDEZ RUIZ, JOSE LUIS (Dirección). Ed. EDERSA. MADRID, 2004. Pág. 179.

184 MARQUEZ LOBILLO, PATRICIA. *Op. cit.* Pág. 180.

> *Parlamento Europeo y del Consejo, de 15 de Diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que son enteramente aplicables a los servicios de la sociedad de la información*[185]*. Dichas Directivas establecen ya un marco jurídico comunitario en materia de datos personales y, por tanto, no es necesario abordar este aspecto en la presente Directiva para garantizar el correcto funcionamiento del mercado interior, en particular la libre circulación de los datos personales entre Estados miembros. La aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso de redes abiertas como Internet.*

De forma análoga, el artículo 1.2 de la LSSICE establece que:

> *Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad nacional, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de las sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.*

En un sentido similar, el artículo 19.2 de la LSSICE, relativo al régimen de las comunicaciones comerciales realizadas por vías electrónica, establece que

> *En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales..*

Hubiese sido deseable la utilización de fórmulas más claras, como la empleada en el texto de la Directiva, que excluye expresamente de su ámbito de aplicación las cuestiones reguladas por las Directivas sobre protección de datos, con el fin de evitar posibles dudas. No obstante, el texto comunitario es tan taxativo que no permite apreciar en la Ley otro sentido que el apuntado por aquél.

---

[185] El concepto de servicios de la sociedad de la información incluye dentro del mismo las operaciones de comercio electrónico, según se determina en el artículo 1.2 de la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de Junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información (modificada por Directiva 98/48/CE). Diario Oficial L 204 de 21-7-1998. Pág. 37.

La aplicación de la regulación sobre protección de datos de carácter personal a los actos de comercio electrónico no implica la aparición de problemas diferentes a los generados por el hecho de la navegación en Internet. Por otra parte, la recogida de datos en los sitios tampoco presenta especialidades que justifiquen un tratamiento separado. Si acaso, ya tratamos alguna de estas cuestiones en líneas posteriores. Quizás, la mayor particularidad que presenta el tratamiento de los datos en el comercio electrónico es la recogida o cesión de las direcciones de correo electrónico para el envío de mensajes publicitarios no solicitados y de forma masiva (spam). Analizamos esta cuestión más adelante, con ocasión del estudio del correo electrónico.

Antes de abandonar este epígrafe, sí quisiéramos recordar algunos aspectos de la regulación sobre protección de datos que se deben tener en cuenta respecto del comercio electrónico. Aunque como ya hemos señalado antes, el concepto de comercio electrónico engloba operaciones que sobrepasan el mero intercambio o adquisición de bienes y servicios, sin embargo, en sentido estricto, aquél supone la celebración de un contrato con dichos fines. Pues bien, debemos recordar que las operaciones de tratamiento que se realizan con ocasión de la celebración de un contrato no requieren el consentimiento del afectado, según establece el artículo 6.2 de la LOPD, a la vez que el artículo 11.2 c) de aquélla exime del consentimiento a las cesiones que se realizan con motivo de una relación jurídica (no sólo negocial o contractual) cuyo control, ejecución y desarrollo exijan la conexión con otros ficheros de terceros. Claro está, tales excepciones se justifican por la existencia de unos supuestos de hecho determinados, que deben concurrir de modo taxativo. Así, la recogida de datos por razón de la celebración de un contrato permite su tratamiento, pero en ningún caso habilita para posteriores cesiones si no se acompaña de dicho consentimiento. Para ellos, la cesión o comunicación debe ser presupuesto necesario del cumplimiento del contrato, según el segundo de los preceptos citados. Además, la excepción al consentimiento del afectado se justifica respecto de aquellos datos que sean necesarios para los fines citados en el artículo 11.2, sin que por ello se justifique el tratamiento inconsentido de la información que tenga carácter secundario respecto de dichos objetivos.

A diferencia de lo que ocurre en el comercio tradicional, en el que los actos de adquisición no suponen obligatoriamente la identificación, por parte del comerciante, del consumidor concreto (supuestos de pago efectivo), las características de la red hacen que en el comercio electrónico sí se consiga dicha identificación. En relación con lo anterior, la utilización de la tarjeta de crédito para realizar compras en la red permite la captación de otro dato de carácter personal, que además da señas de las preferencias y decisiones de compra de los usuarios. Por esta razón, se han articulado medios de pago en la red que funcionen de la misma manera que el metálico en el comercio tradicional: por ejemplo el *digital cash*[186] (dinero electrónico) o

[186] Un de los sistemas de pago anónimo desarrollados es *Digicash*. Se trata de un sistema que se basa en un mecanismo de firma ciega, que utiliza métodos de cifrado o encriptado asimétrico. En efecto, Digicash evita posibles rastreos de la transacción, dado que la entidad bancaria no

el *electronic wallet* (monedero electrónico), que garantizan el anonimato de los consumidores[187]. Alguien podría sostener que la existencia de un contrato entre usuario y oferente a través de la red implica necesariamente la identificación de las partes entre sí. A lo anterior se une la falta de presencia simultánea de las partes. Estas razones justificarían la necesidad de identificación en los actos de adquisición de bienes o servicios. No obstante, como ya hemos dicho en otras ocasiones, el usuario debe recibir el mismo tratamiento que si realizara el acto de que se trate fuera de la red. De esta forma, el pago en efectivo en una adquisición en red elimina la necesidad de identificación, pues la ejecución, y por tanto, la conclusión de contrato ya no justifican la captación de datos de carácter personal, como ocurre en la mera compra de un periódico o de cualquier producto en el medio físico ordinario.

Aunque no queremos extendernos mucho sobre estas cuestiones, pues exceden de objeto de este trabajo, sin embargo sí debemos hacer alguna observación sobre los mecanismos de anonimización en el comercio electrónico. Los métodos antes mencionados de dinero electrónico suponen la intervención de un tercero que, ajeno a la relación entre usuario y comerciante virtual, tiene por misión aportar seguridad a la transacción realizada: únicamente él conoce la identidad del usuario y garantiza a la otra parte que aquél es quien dice ser. Estas *trusted third parties* (en traducción literal, terceras partes confiables) tienen como misión principal otorgar seguridad a las transacciones, evitando que nadie pueda interferir en las mismas y ocasionar perjuicios a los consumidores. Pero también consiguen, a través de estos métodos, evitar la posible identificación del sujeto.

Claro está, estas entidades conocen quien es éste. Por esta razón, resulta necesario garantizar la protección de los datos de carácter personal de los usuarios que poseen estas entidades. En relación con lo anterior, la Ley 59/2003, de 19 de Diciembre, de firma electrónica, establece una serie de prescripciones que deben

---

puede conectar el "dinero" empleado con la cuenta de la que se retiran los fondos empleados. Así, el banco no puede saber qué usuario ha participado en la operación: únicamente lleva control de los "billetes" que se han utilizado.
Otros sistemas, muy empleados hoy en la red para las operaciones que implican utilización de dinero y de cuentas bancarias son SSL o SET, que se basan en el empleo de técnicas de cifrado y de certificaciones digitales de los sujetos que actúan en la operación. No obstante, tal exigencia de certificación impide el anonimato de los usuarios (aunque en algunos casos, como SSL, no siempre se exige esta certificación, lo que puede provocar problemas de identidad real de aquéllos). No pretendemos, no obstante, extendernos sobre estas cuestiones, que, por otra parte, son más propias de un estudio sobre la seguridad en la red, no sólo de la protección de datos de carácter personal.

[187] La Agencia Española de Protección de Datos recomienda el uso de estos mecanismos para garantizar el anonimato. En este sentido, se observa que actualmente existen posiciones favorables, provenientes de voces autorizadas, al mantenimiento de dicho anonimato, en contra de la intención de ciertos operadores en la red y de algunos poderes públicos de exigir la identificación de los usuarios. AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Recomendaciones a usuarios de Internet* (Julio de 1997).

cumplir las entidades certificadoras respecto de la protección de los datos de quienes solicitan sus servicios. Concretamente, dispone el artículo 17 de aquélla:

> *Protección de los datos personales.*
>
> *1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.*
>
> *2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.*
>
> *Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.*
>
> *3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.*
>
> *Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.*
>
> *4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

En definitiva, esta normativa demuestra que la intervención de terceros para garantizar determinados grados de seguridad en las transacciones efectuadas a través de la red, exige que los mismos se sometan a los principios derivados de la legislación sobre protección de datos. Dado que los terceros que participan en la utilización del dinero electrónico tratan de satisfacer fines similares, es correcto exigirles de forma análoga el cumplimiento de dicha normativa.

En realidad, la prestación de servicios de autenticación a los usuarios de la red presupone le tratamiento de sus datos personales. De ahí, que el Grupo de Trabajo del artículo 29[188] ha sostenido la aplicación de la normativa de protección de datos a tales servicios (analiza los casos de net.passport y liberty alliance): determinación de los responsables de los ficheros, empleo de medios de navegación anónima, deber de información, vigilancia de los identificadores, ejercido de los derechos por los usuarios, etc.

También queremos dejar constancia de la perplejidad que nos causa la exigencia de forma expresa al consentimiento para el tratamiento de los datos por parte de las entidades de certificación, cuando se persigan fines distintos al desarrollo del servicio de certificación. Como sabemos, el artículo 7 de la LOPD exige consentimiento expreso para el tratamiento y cesión de los denominados datos especialmente protegidos. Por lo demás, el tratamiento del resto de la información general tan sólo exige, como regla general, consentimiento inequívoco del afectado. Por ello, llama la atención la adopción de un mayor rigor formal por la normativa de firma electrónica. En cualquier caso, la aplicación de esta regla se somete a un criterio finalista (fines distintos al objeto de la actividad de estas entidades). No obstante, la naturaleza de los datos determinará la aplicación de la misma solución, según sean éstos, como hemos señalado. Incluso, se podrá exigir la confirmación escrita del consentimiento en algunos casos, por ejemplo, respecto de los datos de salud. Esta solución se observará en supuestos de contratación por red de servicios sanitarios, de seguros y otros de similar contenido[189].

Antes de abandonar este epígrafe, sí debemos reseñar que las circunstancias económicas inciden en la existencia de numerosos supuestos de cesión o comunicación de datos de carácter personal entre las empresas que ofrecen bienes o servicios por vía electrónica. En efecto, los grandes desembolsos efectuados por estas entidades para su implantación en la red, a lo que se une el lento crecimiento de las operaciones de comercio electrónico, obligan a las mismas a adoptar fórmulas de optimización de recursos que acerquen en el tiempo el umbral de rentabilidad.

Como manifiesta la Agencia Española de Protección de Datos en su Memoria del año 2000, se observan en este sector diversas formas de colaboración[190]. Por ejemplo, es común la utilización de hipervínculos colocados en una página que conducen a una segunda donde se ofrecen productos. Aunque la recogida de datos en la segunda página no tiene porque ir acompañada de la cesión a la primera, sin embargo no siempre ocurre así. Otro método es la oferta de catálogos de bienes o

---

188 Documento de Trabajo sobre servicios de autenticación en línea (adoptado el 29 de Enero de 2003). 100054/03/ES. WP 68. *www.europa.eu.int.*

189 RIBAS ALEJANDRO, JAVIER. *Comercio electrónico en Internet*. En *Problemática jurídica en torno al fenómeno de Internet* (Director. Juan José Martín-Casallo López). Cuadernos de Derecho Judicial. Consejo General del Poder Judicial. MADRID, 2000. Pág. 116.

190 AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria 2000*. Págs. 186 y ss.

servicios de una compañía en la página de otra. En estos casos, la Agencia manifiesta que generalmente ambas entidades acceden a los datos recogidos por la oferente. En tercer lugar, la Agencia cita el caso de la explotación conjunta de contenidos, que ocasiona gran incertidumbre entre los afectados, los cuales desconocen en la mayoría de los casos el destino exacto de sus datos. En este caso, resulta elocuente el ejemplo que la Agencia recoge en la citada Memoria, del cual reproducimos, a continuación, la redacción del texto por su expresividad:

> *En este sentido, la Inspección ha podido verificar la existencia de una página española (ubicada en un dominio registrado por una sociedad nacional con gran implantación en nuestro país) desde la que se recaban datos cuyo destino es una compañía sueca radicada en Chipre, que registró su propio dominio desde Gibraltar y cuyos ficheros se almacenan probablemente en los ordenadores de otra compañía de Gran Bretaña. Sin embargo, en la página correspondiente no se informa acerca de ninguna de estas circunstancias.*

Como se puede observar, la inseguridad provocada por estas cesiones, fruto de la colaboración de las entidades, difícilmente puede ser mayor. Sin que olvidemos, como señala la Agencia, que la ejecución de los contratos electrónicos implica la intervención de empresas del sector logístico que, por lógica, deben conocer alguna información de los compradores. Sin discutir la necesidad de transmitir la información en estos casos, sin embargo sí se debe exigir que la posición jurídica de estas entidades y su responsabilidad queden delimitadas en los clausulados de los contratos electrónicos.

Por todo lo anterior, entendemos que se deben matizar aquellas posiciones que minimizan los riesgos del comercio electrónico, al menos respecto de la protección de datos. Señala Illescas Ortiz que el comercio electrónico es mucho menos intrusivo que el que se lleva a cabo en el mercado real, puesto que los destinos de las comunicaciones comerciales son los ordenadores de los destinatarios, en terminología de la nueva legislación de comercio electrónico. En el comercio tradicional, el aislamiento del consumidor es mayor, el cual no puede desconectarse del mundo real[191]. Aunque la defensa del sector de la contratación electrónica, el cual se encuentra en momentos difíciles, exige una solución que compagine los intereses de cada parte, sin embargo no creemos que las afirmaciones anteriores se justifiquen a la luz de lo anteriormente expuesto.

5.- Los foros de Internet y los datos de carácter personal.

Con la denominación *foro* se hace referencia a uno de los modos de comunicación entre personas a través de Internet que más éxito y desarrollo han experimentado. La escalada en la utilización de aquéllos puede obedecer a varias

---

[191] ILLESCAS ORTIZ, RAFAEL. *Claroscuro con patitos: de nuevo sobre la legislación proyectada en materia de contratación electrónica.* Revista de contratación electrónica, núm. 27. Mayo de 2002. Pág. 13.

razones. En unos casos, se trata de una valiosa herramienta que favorece las relaciones profesionales, dado que permite el intercambio de impresiones, opiniones, documentos, etc. con una gran fluidez. Sin embargo, el motivo principal de su uso es más bien lúdico. Hoy día no hay muchos usuarios de la red que no hayan entrado en uno de estos foros, con el único fin de ocupar el tiempo en una charla intrascendente con personas desconocidas, amparándose en el anonimato para realizar libremente afirmaciones que no haría en un ámbito público. De este modo, podemos encontrar en la red foros sobre materiales de construcción, sobre mercados financieros, a la vez que en otros lugares de la red podemos intentar aumentar nuestro círculo de amistades, fomentar nuestras relaciones afectivas, discutir sobre nuestros cantantes favoritos o recomendar el último restaurante que hemos visitado, entre otros múltiples fines. El interés profesional o el anonimato, según los casos, han provocado que el incremento del uso de estos medios sea exponencial.

Lógicamente tal crecimiento ha venido propiciado por la propia oferta de los operadores. No existe portal de Internet que no ofrezca un servicio de *chat* (charla electrónica) a sus usuarios. Los beneficios generados no son despreciables: los operadores de telecomunicaciones incrementan su facturación, sobre todo respecto de los foros sobre temas generales, a los cuales se conecta muchos usuarios sin motivo aparente. Los servidores aumentan la navegación a través de los mismos. Los portales aumentan en número de usuarios, lo que les posibilita un aumento en la facturación por publicidad. Curiosamente, la utilización de estos foros se vuelve compulsiva en aquellos casos en los que se accede de forma frívola e insustancial. Además, se han ampliado los modos de acceso con la posibilidad de *chatear* desde los teléfonos móviles, lo que principalmente afecta a la población en edad adolescente.

No obstante lo anterior, no es el beneficio económico obtenido de forma directa el único objetivo de estos foros. Por su propia naturaleza, se trata de espacios públicos donde los usuarios vierten sus opiniones sobre temas variados, cuando no incurren en la irresponsabilidad de manifestar cierta información que, de modo más o menos directo, hace referencia a sus señas personales. En este sentido, los foros se han convertido en un medio de discriminación e identificación de caracteres personales, cuando no la captación directa de datos identificativos. El peligro que para la protección de los datos de carácter personal representan aquéllos, es quizás mayor que en otros casos. A la ignorancia generalizada, propia de todos los medios que ofrece Internet, se une la citada la falta de trascendencia que mueve a los usuarios en estos casos, lo que provoca que su atención respecto de su privacidad se relaje y pase a un segundo plano. Los usuarios olvidan que su anonimato, en estos foros de carácter público, depende exclusivamente de sus actos, desconocen que existen poderosos medios técnicos que vigilan todas sus afirmaciones y expresiones, a la vez que generalmente sólo se preocupan del desarrollo de la conversación que sostienen en un momento con otro u otros usuarios. Psicológicamente, se predisponen al olvido de su privacidad.

Como hemos señalado, estos foros son públicos. Tal circunstancia podría hacer pensar que la información recogida de los mismos no está protegida por la legislación sobre protección de datos, dado que la misma procede de fuentes públicas en las que se ha depositado voluntariamente tal información. De esta forma, los usuarios, negligentes o ignorantes, se verían totalmente desprotegidos, a merced de los intereses empresariales. Como afirma el Grupo de Trabajo[192], la protección que brinda tal regulación se mantiene una vez que los datos han sido publicados y han pasado a ser de posible conocimiento general. Se debe tener en cuenta que la publicación de tales informaciones únicamente rebaja el rigor o las exigencias que la normativa impone respecto del tratamiento de estos datos. Pero en ningún caso se establece por aquélla que estos datos sean excluidos de su ámbito de aplicación.

Un ejemplo claro de lo anterior es la configuración, por la LOPD, del Censo Promocional como fuente accesible al público y la aplicación de una serie de preceptos al mismo, si se quiere, más flexibles. De ahí que debamos analizar esta figura de los foros para señalar cuáles son las soluciones jurídicas que se deben adoptar respecto de los mismos. Debemos partir de la circunstancia de que en estos casos concurre el consentimiento de los usuarios, lo que rebaja mucho las exigencias de quienes tratan los datos. Sin embargo, también se debe analizar qué extensión tiene dicho consentimiento, pues de la misma dependen en gran medida las posibilidades de los últimos.

a. Los distintos foros públicos.

Sin ánimo de ser demasiado exhaustivos, sí conviene reseñar alguna de las características de los diferentes foros existentes en Internet. Generalmente, se suele distinguir entre los foros de debate y las charlas electrónicas. Los primeros, también conocidos como *newsgroups*, suelen tener carácter temático, de manera que los usuarios hacen aportan sus opiniones y responden a las de otros sobre un tema concreto. Dichas manifestaciones pueden ser leídas por personas que no pertenecen al foro. Además, toda la información vertida por este cauce se almacena durante un período de tiempo, con la finalidad principal de que los usuarios puedan consultar la misma. En estos foros es muy común que los artículos publicados sean intercambiados o cedidos entre los servidores a que pertenecen los distintos foros.

Quizás los foros más utilizados y conocidos sean las charlas electrónicas, los llamados *chats*. Básicamente, se trata de un servicio en virtud del cual dos o más personas se pueden comunicar en tiempo real entre ellas utilizando un espacio destinado a ello. Todos las manifestaciones que los usuarios hacen en estos espacios pueden ser conocidos por todos los usuarios conectados al chat, salvo en aquellos supuestos en los que dos usuarios abren una vía separada de comunicación, en la que excluyen a los demás participantes de la misma.

---

[192] *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*…Pág. 60.

Por su configuración técnica, los chats se clasifican en: IRC (charla interactiva), que tiene características similares a los foros, con la diferencia de que terminado la charla se cierran las conexiones; charla en página web, que supone la navegación por red para acceder a una página en la que se desarrolla la charla (en el caso anterior se utiliza un programa específico de chateo) y charla ICQ, que permite navegar a la vez que se conversa y saber quienes están conectados. La segunda de las versiones es la más utilizada por su simplicidad, dado que solamente requiere la conexión a la red y el navegador, que lógicamente se posee, sin necesidad de conocer y utilizar otras aplicaciones. Por supuesto, este tipo de charlas permite a los portales y proveedores de servicios tener mayor control sobre las manifestaciones aparecidas en aquéllas, dado que la *tertulia* se desarrolla en su seno.

b. Los tratamientos y cesiones de los datos incluidos en estos foros.

El principal riesgo que suponen para la privacidad estas charlas o foros es su carácter público, la posibilidad de conocimiento generalizado. La consecuencia inmediata que más nos interesa a este respecto es la posibilidad de numerosas cesiones y consiguientes tratamientos de la información recabada en aquéllos. En este sentido, dicha información se puede recoger de dos formas: una originaria, mediante la contestación a un formulario que el responsable del chat solicita al usuario que pretende acceder al mismo. En este caso, se trata de datos personales que posteriormente son de conocimiento general en algunos casos: por ejemplo, el artículo de un foro suele ir acompañado de la dirección de correo electrónico, en los chats se ofrecen a quien desea acceder, perfiles de los usuarios conectados.

A lo anterior hemos de unir que en muchas ocasiones, los chats unen al seudónimo utilizado por los usuarios la dirección IP de los mismos. Los responsables suelen afirmar que la finalidad de recoger tal información es doble: control de las afirmaciones vertidas, como forma de exoneración de responsabilidad, y elaboración de listas de datos. Pues bien, esta última finalidad implica la realización de cesiones o comunicaciones de los datos recogidos. En efecto, existen hoy potentes buscadores en la red que permiten la captación de toda la información que se puede conectar, utilizando diferentes criterios de búsqueda, a una persona[193]. También se pueden captar datos personales mediante el empleo de troyanos que permitan el acceso al

[193] Resulta preocupante, más que curioso, observar la información que sobre uno mismo se puede encontrar en Internet con realizar la sencilla operación de incluir su nombre en un buscador (por ejemplo, Google). Si es poca la inquietud que pueda generar el hecho de que se pueda averiguar su profesión y ubicación del lugar concreto de trabajo, al aparecer en la página de la empresa o institución, no ocurre lo mismo, sin embargo, cuando se observa que también se está incluido, por ejemplo, en la publicación de los edictos de una entidad recaudatoria de una Administración por impago. No olvidamos que la finalidad de aquéllos es precisamente la publicidad, la cual aumenta con el uso de Internet. No obstante, los posibles usos de esta información pueden no estar justificados.

equipo por otro participante del chat, cuando se emplea el sistema IRC[194]. En definitiva, tales herramientas realizan una operación de recogida similar a la que cualquiera puede hacer cuando consulta una base de datos de un colegio profesional o el Censo electoral. Sin embargo la potencia de recogida y el acceso generalizado a la ya captada hacen que el conocimiento y el tratamiento de los datos puedan ser indiscriminados, lo cual resulta difícilmente justificable, incluso de datos provenientes de fuentes públicas.

Diferentes organismos internacionales[195] han hecho hincapié en la necesidad de reforzar la posición jurídica de los usuarios que acceden a estos servicios. Concretamente, se ha reclamado el cumplimiento de una serie de medidas derivadas de la legislación sobre protección de datos a los portales y servidores. La mayoría de estas medidas hacen referencia a la obligación de proporcionar variada información sobre los diferentes extremos que pueden afectar a la información de los usuarios: integridad y confidencialidad de la información, tratamiento leal, consentimiento explícito, período de almacenamiento, entre otros deberes. Efectivamente, tales exigencias poseen un carácter preventivo, dado que su cumplimiento inicial otorga a los usuarios mayor responsabilidad en sus actos. Sin embargo, a nosotros nos interesa determinar que exigencias tienen los responsables de tales espacios una vez que los datos ya han sido recabados y pueden ser objeto de cesión.

Según el artículo 11 de la LOPD, la cesión de datos de carácter personal provenientes de fuentes accesibles al público no requiere la concurrencia del consentimiento del afectado. Ahora bien, tales cesiones deben sin embargo satisfacer el cumplimiento de los fines legítimos de cedente y cesionario, según el párrafo 1º de dicho precepto. Se trata de un requisito que se debe satisfacer en todo caso, sea cual sea el origen de los datos. Como señala el artículo 4 de la LOPD, los datos no podrán ser tratados para satisfacer fines distintos de aquéllos que motivaron su tratamiento, a la vez que el mismo precepto consagra el principio de lealtad, según el cual no podrán tratarse datos que no sean pertinentes con los fines propuestos. De lo anterior se puede colegir, por tanto, que los datos no pueden ser cedidos para fines distintos de los que justifican su recogida y almacenamiento. Difícilmente los fines del cesionario se tienen en cuenta a la hora de recabar los datos de los usuarios, por lo que su coincidencia con los objetivos iniciales es más que dudosa. Dicho de otra forma, el mantenimiento de los fines en todos los posibles tratamientos por parte de quien recoge los datos, los cuales se manifiestan inicialmente al usuario, exige que esos fines que pretendan satisfacerse se observen también en el momento de la cesión y que, por supuesto, se comuniquen a éste último.

---

[194] RIBAS ALEJANDRO, JAVIER. *Op. cit.* Pág. 159.

[195] Por ejemplo, el Consejo de Europa en la Recomendación R (99) 5 sobre protección de la privacidad en Internet. En sentido similar se han pronunciado organizaciones como W3C, EPIC, etc.

En relación con la exigencia de la legitimidad de los fines de las operaciones de tratamiento, existen algunas dudas de que el objetivo de control justifique dichas operaciones. No cabe duda que los foros y los chats pueden ser utilizados con fines ilícitos, cuando no delictivos. Ahora bien, la posibilidad de tales usos nocivos no permite un control apriorístico y general de todas las posibles intervenciones que se recogen en tales espacios, así como de los sujetos que las realizan. Como ha señalado el Grupo de Trabajo en la Resolución 3/97, sobre el Anonimato en Internet[196],

> *… Análogamente, no obstante, la capacidad de los gobiernos y Administraciones públicas para restringir los derechos de las personas y controlar las actuaciones potencialmente ilícitas no debería ser mayor en Internet que en el mundo exterior, no automatizado. La exigencia de que las restricciones de los derechos y libertades fundamentales estén debidamente justificadas y sean necesarias y proporcionadas a otros objetivos de orden público deben cumplirse también en el ciberespacio.*
>
> *El principio conforme al cual el régimen aplicable a Internet no debe ser más o menos favorable que el aplicable a tecnologías más antiguas está recogido tanto en la introducción de la Comunicación de la Comisión sobre contenidos ilícitos y nocivos en Internet, donde se afirma que "lo que es ilícito fuera de línea lo es también en línea", como en el informe del Grupo de Trabajo sobre contenidos ilícitos y nocivos en Internet, que en su segunda propuesta de acción futura establece el principio de que "deberá otorgarse el mismo grado de libertad de circulación a la información que se transmite por Internet que la que se difunde en papel".*

Efectivamente, la mayor fluidez que los mecanismos analizados otorgan a las comunicaciones entre personas, no justifica la posibilidad de que los controles, restrictivos de los derechos fundamentales de aquéllas, puedan realizarse sin garantía alguna de los mismos. El establecimiento de medidas de control previo a la comisión de actos ilícitos, con carácter preventivo, elimina la aplicación del principio de proporcionalidad que el TEDH exige, como hemos visto, para la interceptación y, por tanto, el conocimiento por cualquier persona ajena a la comunicación del contenido de la misma.

Las particulares características del medio empleado para la comunicación no constituyen un presupuesto suficiente de la legitimidad de dichos controles. De aquí, que el Grupo de Trabajo proponga, con toda razón a nuestro parecer, la adopción de un régimen jurídico aplicable a estos servicios de Internet, como a otros, que sea análogo al empleado en servicios similares prestados fuera de la red. Carece de la más elemental lógica que alguien goce de la privacidad suficiente para ejercer su

---

196 GRUPO DE TRABAJO SOBRE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Recomendación 3/97, sobre Anonimato en Internet* (3 de Diciembre de 1997). XV D/5022/97 ES final.

derecho de libertad de expresión en un tablón y sin embargo no tenga las mismas posibilidades en la red.

Como soluciones al problema planteado, se ha propuesto que los servidores que alojan los servicios de chat y news permitan a los posibles usuarios la utilización de seudónimos previamente otorgados por servidores especializados en estas tareas. De esta forma, el usuario accedería al foro de forma anónima. Nosotros pensamos que la misma función podría y debería desarrollar el servidor que aloja estos servicios, con el fin de evitar que la complicación de dichos actos tenga un efecto disuasorio en los usuarios. Frente a esta opción, se ha argumentado que la anonimización puede ir en contra de la eficacia en la persecución de los actos ilícitos. No obstante, resulta obvio que tales servidores podrían arbitrar algún mecanismo que les permitiese mantener la posibilidad de enlazar un seudónimo con la persona a quien pertenece, cuando justifique por motivos de seguridad u orden públicos tal medida. En algunos servidores se utiliza un mediador o moderador que vigila el contenido de los mensajes, como modo de exonerarse responsabilidad alguna por los contenidos. No tenemos, en principio, nada en contra de esta posibilidad, siempre, claro está, que se permita y garantice a los usuarios mantener su anonimato, pues tal vigilancia impide la responsabilidad derivada de la ilicitud de tales contenidos, por lo que tal control hace innecesario el control sobre los sujetos.

Por otra parte, el carácter público de los foros y los chat no implica necesariamente la excepción a la necesidad de consentimiento de los afectados a las cesiones o comunicaciones de sus datos. Si en efecto los listados de datos extraídos de estos foros son de acceso público, no parece sin embargo que, como consecuencia necesaria de lo anterior, deban ser considerados fuentes accesibles al público. La inclusión en el artículo 3 de la LOPD de una lista cerrada de tales fuentes, exige que la misma sea interpretada en sentido estricto, como medio de proteger la posición de los afectados. De la citada lista no se deduce en ningún caso que los listados de afectados o usuarios participantes en foros o chat sean fuentes accesibles al público. Por lo tanto, las cesiones de los datos contenidos en dichos listados publicados (no tanto públicos) requieren consentimiento previo del usuario. Esta afirmación se refuerza por la exigencia de que el fin sea legítimo, pues tal legitimidad se adquiere por la concurrencia del consentimiento, según establece el artículo 7 de la Directiva 95/46, entre otras exigencias.

Así, en la Recomendación del Grupo de Trabajo del artículo 29 sobre determinación de los requisitos mínimos para la recogida en línea de los datos personales en la Unión Europea[197], se afirma textualmente que *no es lícito recopilar direcciones electrónicas en áreas públicas de Internet, como foros o grupos de debate, sin conocimiento del interesado. Por lo tanto, estas direcciones no se podrán usar para una finalidad distinta de aquélla para la cual se han hecho públicas, en especial, el márketing directo.* Aunque podría pensarse que las anteriores palabras sólo exigen información, que no voluntad acorde del

[197] *Vid.* nota 76.

usuario, sin embargo continúa el Grupo de Trabajo manifestando lo siguiente: *el uso de las direcciones electrónicas para márketing directo exclusivamente cuando se hayan recopilado de manera leal y lícita. Le recogida leal y lícita implica que los interesados han recibido información sobre la posibilidad de que sus datos se utilicen con fines comerciales de márketing directo y se les ha dado la opción de aceptar dicho uso directamente en el momento de recoger la información (casilla de aceptación en línea).* Como se puede comprobar, se recuerda la necesidad de contar con el consentimiento del usuario para la recogida y tratamiento de dicho datos.

En relación con lo señalado anteriormente, conviene afirmar la nítida distinción entre las guías de abonados y los directorios o listados que de las direcciones de correo electrónico, entre otros datos, aparecen en páginas destinadas a prestar un servicio de news o chat. Podría sostenerse que tales listados facilitan la comunicación, en este caso por red, entre los usuarios de la misma. Así, la finalidad de aquéllos sería similar a la de las guías telefónicas. No obstante, las diferencias son apreciables. Por un parte, se trata de un dato de carácter personal diferente al número de teléfono y la dirección. Además, la generalización del uso del teléfono facilita la consideración de medio de interés general de las guías, característica que no concurre en estos directorios electrónicos. Otra diferencia radica en el modo de recogida de los datos, dado que los listados de la red no gozan de la publicidad y el acceso general de las guías, por lo que los usuarios no tienen conciencia de que sus datos figuran en tal o cual sitio web. Quizás por todos estos argumentos la LOPD recoge, en la lista cerrada del artículo 3, las guías telefónicas como fuentes accesibles al público, sin hacer mención alguna de otros ficheros análogos. No es necesario recordar que la corrección jurídica impide la aplicación analógica de una norma de carácter restrictivo, como forma de proteger, en este caso, la posición de los afectados.

Lo anterior no es compatible con una equiparación de la posición jurídica de los usuarios telefónicos y de la red, concretamente de los derechos que les asisten, como han afirmado algunos[198]. Tal posibilidad supone que, aparte de los derechos de exclusión, de prohibición del uso de los datos para fines de venta directa, de omisión parcial de la dirección y de eliminación de referencia alguna al sexo, los usuarios de red que figuren en los listados deben consentir la inclusión de datos personales que no sean necesarios para su identificación, por lo que no es necesario que concurra su voluntad en caso contrario. Por lo tanto, los directorios de direcciones de correo electrónico que sólo contienen éstas no requieren consentimiento del afectado.

Sin embargo, las diferencias en la naturaleza y el tratamiento jurídico de las guías telefónicas y los directorios de la red citados, impiden esta asimilación. Al no ser fuentes accesibles al público, los últimos no pueden incluir los datos de los usuarios sin que los mismos se hayan recabado con su consentimiento.

---

198 CORRIPIO GIL-DELGADO, MARIA DE LOS REYES. *Regulación jurídica de los tratamientos de datos*… Pág. 219.

Consentimiento que efectivamente puede ser expreso o tácito, pero consentimiento al fin y al cabo, pues es necesario que concurra una solicitud en tal sentido, a diferencia de lo que ocurre en el caso de las guías telefónicas. En relación con esta cuestión, el artículo 30 de la LOPD establece que la recopilación y tratamiento con fines de publicidad de datos de carácter personal requieren que los mismos se extraigan de fuentes accesibles al público o, en caso contrario, que el afectado haya prestado su consentimiento. La correcta aplicación de este precepto requiere una interpretación restrictiva de dichas fuentes que excluya la posibilidad de incluir listados no mencionados expresamente, eliminando virtualmente la exigencia del consentimiento en muchos de estos supuestos. No es posible, por tanto, ni la asimilación conceptual ni la consiguiente equiparación de las consecuencias jurídicas para los afectados.

6.- Los datos de carácter personal y el correo electrónico.

El correo electrónico o *e-mail* es, quizás, el servicio prestado a través de Internet que más se ha popularizado[199], por las virtudes que representa para la comunicación interpersonal. El correo electrónico permite a su usuario remitir mensajes a uno o varios destinatarios. Entre las ventajas que posee, la primera y más destacable acaso sea la rapidez del envío. Sin embargo, la fluidez del medio se puede obtener mediante una llamada telefónica. En efecto, en el correo electrónico acompañan, a dicha agilidad, otros beneficios.

a. El esquema técnico.

En primer lugar, su configuración técnica permite evitar el inconveniente de que el destinatario del mensaje no se encuentre en el momento adecuado en disposición de conocer el mensaje, como veremos a continuación. Así, el mensaje puede ser enviado y depositado en el servidor correspondiente, de modo que el destinatario podrá consultarlo cuando considere oportuno. Además, la utilización de las mismas vías que la navegación por Internet hace que la conexión no sea continua, con lo que se evita igualmente la posibilidad de que el destinatario esté comunicando con otros usuarios.

---

[199] Dicho éxito ha comenzado a ser preocupante en el sector empresarial. En efecto, tanto en E.E.U.U. como en Europa se ha producido un vertiginoso aumento del correo electrónico facilitado por la empresa a los trabajadores. En la mayoría de los casos, la utilización del mismo parece realizarse con fines exclusivamente personales, no relacionados con el desempeño de las actividades objeto de la relación laboral. Concretamente, en España los intentos de las empresas por frenar este uso fueron objeto de litigios en la jurisdicción laboral, que, en algunos casos, dieron la razón al trabajador en defensa de su derecho a la intimidad o a la libertad sindical. Igualmente, la Agencia Española de Protección de Datos ha sancionado tales actos en algunos casos (por ejemplo, al Grupo Recoletos).

Otra de las características que han provocado el auge de este correo es la enorme variedad de contenidos que puede acoger. Si bien en la mayoría de los casos los correos contienen mensajes de texto, sobre innumerables cuestiones (profesionales, personales), sin embargo también se usa de forma ingente para el envío de archivos de texto elaborados previamente (un informe, una felicitación navideña, un programa de cualquier tipo de evento, un virus,…), archivos de audio (una canción), de vídeo (una presentación de un producto, un corto de una película, un chiste…) y demás posibilidades. De esta forma, el correo electrónico no sólo sustituye, en lo posible, el tradicional correo de cartas, sino que afecta al negocio de paquetería. La comodidad de este medio, unida a la reducción de costes en el sector empresarial y público, justifican su éxito.

El esquema técnico del correo electrónico es relativamente sencillo. El vehículo electrónico obliga a la participación de unos intermediarios que facilitan el transporte. De esta forma, los participantes en dicho proceso son: el remitente, el destinatario y los proveedores de servios de correo o servidores de correo electrónico. A diferencia del correo tradicional, en este caso no es el mismo operador el que se encarga de que el mensaje salga de su origen y llegue a su destino, sino que cada parte del mensaje tiene un servidor que facilita uno de los dos pasos. Cada uno de estos sujetos necesita tener instalados en sus equipos aplicaciones o programas de correo. Por otra parte, la utilización de medios electrónicos e informáticos exige la utilización de un lenguaje o protocolo que permita a los equipos entenderse entre sí. De esta forma, en el correo electrónico se utilizan dos protocolos: el protocolo SMTP y el POP. El primero es el que se utiliza para llevar a cabo el envío del mensaje (protocolo de correo saliente). El segundo es que permite al destinatario conectar con su servidor de correo para reclamar la recepción del mensaje (protocolo de correo entrante).

El proceso básico de un mensaje de correo electrónico es el siguiente: quien desea remitir un mensaje utiliza su programa de correo. Tal programa le facilita un esquema del mensaje en sí (tales formatos presentan pocas diferencias, según el programa escogido), en el que aquél detalla la dirección de correo del destinatario, su propia dirección (aunque tal circunstancia no necesariamente debe concurrir, como veremos), una mínima descripción del contenido (si así lo desea) y, por supuesto, el mensaje en sí. Una vez escrito, se envía el mensaje, no al destinatario de forma directa, sino que el mismo se recibe por el servidor de correo de aquél. De esta forma, si el destinatario desea conocer el contenido del correo, deberá acceder a su servidor, mediante la inclusión de un nombre usuario y una contraseña, para poder abrir su correo. Es decir, cada usuario de correo electrónico tiene un *buzón* en el que el servidor deposita los mensajes que van dirigidos al mismo.

Claro está, para que los mensajes puedan ser recibidos por su destinatario, es imprescindible que el mismo se identifique. En el medio electrónico, tal fin se consigue mediante las cuentas de correo electrónico. Estas direcciones presentan el mismo esquema: la primera parte hace alusión a la identificación concreta del usuario (puede ser su nombre y/o apellidos o puede utilizar, como generalmente

ocurre, nombres falsos o anónimos, lo cual resulta bastante interesante, ante las grandes posibilidades que actualmente existen de captación de tales datos en la red). A continuación aparece el símbolo @, descriptivo del uso del correo electrónico. La tercera parte de la dirección está compuesta por el nombre del servidor de correo de dicho usuario. Por ejemplo, *pepe@fcjs.urjc.es* nos indica que se trata de una cuenta de correo, que su usuario *se identifica* por Pepe y que el servidor pertenece a la Facultad de Ciencias Jurídicas y Sociales de la Universidad Rey Juan Carlos.

El proceso descrito anteriormente se refiere a la manera más común de uso del correo electrónico. Sin embargo, en muchas ocasiones las cuentas de correo están asociadas o vinculadas a una empresa, un organismo, una entidad, etc. en que se desarrolla la actividad laboral. En estos casos, los equipos terminales están conectados de forma permanente a sus servidores, de forma que la remisión del mensaje es automática. Aunque en muchos de estos casos se exijan contraseñas para evitar posibles accesos indebidos, no es necesario conectar previamente con el servidor de correo.

Por otra parte, muchos usuarios de Internet utilizan el correo web. Se trata de una variante de correo electrónico que utiliza el sistema de páginas o sitios de Internet. En estos casos, tales sitios ofrecen a los usuarios la posibilidad de crear una cuenta de correo en dicha página. De esta forma, el usuario evita tener que contar con un programa de gestión de correo, puesto que en realidad lo que hace es acceder a una página, en la que se ha habilitado un espacio de memoria para que éste reciba los mensajes. Funciona de forma similar a los apartados de correos, puesto que el mensaje no llega hasta nuestro ordenador, sino que somos nosotros quienes acudimos a la página para verlos en la misma. Este sistema es muy utilizado como correo estrictamente personal, pues evita el inconveniente de tener que recibir el mensaje en el propio ordenador (que muchas veces es el del lugar de trabajo) para tales fines, a la vez que se trata de un servicio prestado de forma gratuita.

Cualquiera que sea la fórmula empleada para el envío de los mensajes de correo, se trata de un medio de comunicación que, por tanto, recibe la protección del secreto de las comunicaciones del artículo 18.3 de la Constitución. En efecto, la Constitución protege aquéllos con independencia de los elementos técnicos empleados y de la facilidad fáctica para la interceptación: tal facilidad no conlleva, lógicamente, su posibilidad jurídica. Así, es aplicable lo dicho en el capítulo anterior respecto del objeto de la protección de este derecho en relación con los correos electrónicos. Señala Fernández Esteban que, sobre la base de la expectativa del secreto, según la cual el artículo 18.3 protege aquellas informaciones que las partes no desean divulgar y presuponen su secreto, no forman parte de la comunicación las partes de las mismas fácilmente visibles[200]. Así, se puede afirmar que aquellas partes no visibles forman parte de la misma, *sensu contrario*.

---

[200] FERNANDEZ ESTEBAN, MARIA LUISA. *Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las comunicaciones entre particulares, en especial en el ámbito de la empresa.* Aranzadi Civil, núm. 3. Mayo de 2000. Pág. 1890.

b. La consideración de la dirección de correo electrónico como dato de carácter personal.

El uso del correo electrónico plantea diversos problemas en relación con la protección de datos de carácter personal. Por ejemplo, la utilización del mismo a través de la red posibilita operaciones de tratamiento invisible de los datos, ya analizadas; igualmente, el envío de mensajes genera, pues en sí mismo es una comunicación, datos de tráfico; el contenido del mensaje puede contener información personal, que puede ser interceptada; las direcciones de correo son objeto de recopilación en la red e inclusión en repertorios. Todo lo anterior se fundamenta, claro está, en la configuración de la dirección de correo electrónico como un dato de carácter personal, por cuanto hace referencia a una persona identificada o identificable.

En efecto, la dirección puede dar noticia directa de la persona titular de la misma o indicar de forma indirecta cuál pueda ser ésta (cuando se emplean seudónimos y las operaciones de tratamiento permiten la conexión de la dirección con un sujeto concreto). La mayoría de las opiniones sobre esta cuestión, conforme se deduce de la legislación sobre protección de datos, son acordes con la naturaleza personal de la dirección de correo electrónico[201], siempre que concurran las circunstancias mencionadas. En sentido, merece destacar la opinión de Aparicio Salom al respecto[202]. Según este autor, la dirección de correo sólo se puede considerar

---

[201] Así lo afirma, por ejemplo, la CNIL (Commission Nationale de l´Informatique et des Libertés), autoridad de control francesa, en su informe sobre el correo electrónico. Señala este organismo que, aunque la determinación del sujeto sólo pueda ser indirecta, sin embargo se trata de una dato que siempre va asociado a un nombre y a una dirección física. En realidad, de una dirección de correo electrónico se pueden deducir varios datos de carácter personal: su nombre, su dirección profesional, entre otros. CNIL. *Le publipostage électronique et la protection des données personnelles*. Se puede encontrar en http://www.cnil.fr/ . En este sentido la Comisión del Senado sobre redes informáticas, ha afirmado que el domicilio electrónico de una persona forma parte de su vida privada y es inviolable. Lógicamente, este tratamiento del domicilio electrónico implica que la dirección de correo electrónico, que ubica tanto a la persona titular del mismo como al equipo desde el que se obtienen o envían los mensajes, se considere un dato de carácter personal. *Acuerdo del Pleno del Senado por el que se aprueba el Informe de la Comisión especial sobre redes informáticas*. Págs. 45 y 46. Boletín Oficial de las Cortes Generales. Senado. VI Legislatura. Serie I: Boletín General de 27 de Diciembre de 1999. Núm. 812. Este documento se puede encontrar en http://www.senado.es/.

[202] APARICIO SALOM, JAVIER. *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal*. Ed. Aranzadi. Elcano (navarra) 2000. Págs. 43 a 47. En el mismo sentido, AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 2000*. Pág. 338. No obstante, la postura del citado no ha sido siempre la misma, como vemos a continuación.
En otro sentido, CORRIPIO GIL-DELGADO (*Op. cit.* Págs. 68 y 69) sostiene que el correo electrónico posee una naturaleza dual, como correspondencia y como dato de carácter personal. En efecto, estas direcciones pueden formar parte del proceso de la comunicación y

dato de carácter personal cuando la misma se asocie a una persona como consecuencia de una operación de tratamiento que vincule la información con la persona. Sobre la base del concepto de dato de carácter personal que recoge la LOPD, la información es el dato en sí, mientras que su carácter personal resulta de su vinculación al sujeto por medio de las operaciones de tratamiento. En un sentido similar se pronuncia la Agencia Española de Protección de Datos, según la cual la consideración de la dirección como dato de carácter personal requiere la vinculación del dato al sujeto. No obstante, aunque la Agencia reconoce, como no puede ser de otra manera, la necesidad de conexión entre el dato y su titular, sin embargo entiende, a mi modo de ver de forma acertada, que tal requisito no implica necesariamente el uso de una dirección en la que se incluya datos identificativos de dicho sujeto. Añade, además, que el tratamiento de las direcciones está supeditado al consentimiento de los afectados, sin que se pueda argumentar el carácter público de tales datos[203]. También afirma que en los casos en los que la dirección no muestre de forma directa datos personales, sin embargo la referencia a un dominio concreto implica la posibilidad de identificación a través de la consulta al servidor[204].

Estamos plenamente de acuerdo con la necesidad de la vinculación a una persona de la información para que la misma pueda revestir el carácter de personal. Ahora bien, ello no quiere decir que tan solo las direcciones de correo electrónico que contiene los verdaderos nombres de sus titulares puedan revestir tal carácter. Por el contrario, el carácter aparentemente anónimo de una dirección se puede romper con facilidad, por la contestación sincera de los cuestionarios de la cuenta de correo, por la conexión de la utilización del correo con otras operaciones del usuario en la red en la que se identifica; por el agotamiento del usuario, que ya no desea seguir mintiendo, etc. En todos estos y otros casos, la desvinculación de la dirección y la persona titular de la misma no se mantiene de modo indefinido. De ahí, que existan muchas posibilidades de que tales usuarios sean identificables, sino identificados.

En este mismo sentido, la Agencia Española de Protección de Datos ha llegado más lejos en sus afirmaciones. Incluso, en consonancia con lo señalado en líneas anteriores, en los supuestos en los que no se produce la identificación del sujeto,

---

de su contenido, lo que las incluye en el ámbito de protección del artículo 18.3 de la CE. En este caso, sólo nos interesa su configuración como dato de carácter personal, sin perjuicio del análisis del ámbito del artículo 18.4 y sus relaciones con el párrafo 3º del mismo precepto constitucional.

[203] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 2000*. Págs. 338-339. Dicha doctrina ha sido manifestada en repetidas ocasiones por la Agencia o por alguno de sus componentes. Así se pronunció Rubí Navarrete, Adjunto a la Dirección de la Agencia Española de Protección de Datos, en la Conferencia de autoridades de protección de datos de Estocolmo (Abril de 2000). La propia Agencia había manifestado esta posición en la Memoria del año 1999.

[204] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Informe sobre la dirección de correo electrónico*. www.agpd.es.

lo cierto es que las direcciones de correo electrónico pertenecen a un sujeto que puede ser identificado en virtud de los ficheros que se contienen en el servidor de correo a quien pertenece el dominio, que aparece como segunda parte de la dirección, según ya vimos[205]. Como ya se ha reseñado en repetidas ocasiones, se considera dato de carácter personal cualquier información sobre persona identificada o identificable, circunstancia esta última que concurre en las direcciones de correo electrónico.

La consideración de la dirección de correo electrónico como un dato de carácter personal, se deduce de la protección que en el mismo recibe en diversos pasajes de la Directiva 2002/58, por ejemplo, en el artículo 13, relativo a las comunicaciones no solicitadas.

c. El tratamiento de las direcciones de correo electrónico.

Los tratamientos más comunes de las direcciones de correo son las que se producen como consecuencia de la utilización de los programas de correo, así como las que, con posterioridad a la captación de aquélla, los sitios web remiten a terceros. En el primer caso, se trata de un supuesto de tratamiento invisible. De esta forma, cuando se utilice dicho programa, puede ocurrir que se transmita la dirección al sitio del titular de dicho programa de forma involuntaria, debido a la inclusión de un código en el primero. Igualmente, en el correo web la dirección se puede captar mediante la inclusión de hipervínculos invisibles, que la remiten a terceros de forma inconsentida. En realidad, se trata de supuestos ya estudiados, con la única diferencia de que se surgen con ocasión del uso del correo, no en una sesión de navegación.

En segundo lugar, hoy día resulta común la utilización con fines económicos de los datos de carácter personal recabados por los sitios web. Concretamente, han proliferado las operaciones de cesión de dicha información a terceros, generalmente a través de una venta, así como la remisión de la misma a empresas de análisis de marketing[206]. Sin pretender alargarnos mucho con esta

---

[205] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Memoria del año 1999*. Págs. 406 y ss.

[206] La comercialización de los listados de direcciones de correo electrónico se suele hacer mediante operaciones de corretaje de las empresas de marketing o por la celebración por éstas de un contrato para llevar a cabo una campaña. Generalmente, los servicios que se prestan en estos casos son: el arriendo de los datos, la inclusión de un vínculo en el mensaje publicitario que conecte con la empresa que se anuncia, el recuento de las veces que se utiliza este hipervínculo para acceder a la página del anunciante (lo que se denomina pulsaciones pasantes o *click through*) y, finalmente, la comprobación del nivel de éxito de la campaña. El precio de tales actividades se medía, en épocas anteriores, por el número de correos enviados: 200 dólares por cada 1000 mensajes (en Europa, no existen criterios claros y generales sobre el coste de estos servicios), a lo que se debe añadir el coste de realizar tales envíos atendiendo a una serie de criterios concretos: zona, operaciones de comercio electrónico realizadas, edad, estado civil, etc. Sobre estas cuestiones, consultar el informe elaborado para la Comisión

cuestión, sí tenemos que recordar que el sitio web que recoge los datos, deberá, como cedente de los mismos, haber obtenido el consentimiento del usuario (que puede ser tácito si, previamente requerido para negarse a consentir tales cesiones, el usuario no se opone: es lo que se conoce como *opt-out*) para dicha operación, previa información al respecto en el mismo momento de la recogida u otro momento posterior, en cumplimiento de lo dispuesto en los artículos 11 y 5 respectivamente de la LOPD y preceptos concordantes de la Directiva 95/46. La solución más común en la práctica es que en el clausulado adjunto al formulario de datos personales se incorpore una mención a la posibilidad de los tratamientos[207].

No obstante, tenemos que puntualizar que estas cesiones no se matizan por la especialidad del medio de transmisión. En realidad, se trata de datos cedidos por medios tradicionales: si acaso la citada especialidad se observa en el momento de la recogida de los datos, no en el posterior de la cesión. En este sentido, su realización deberá satisfacer los mismos requisitos exigidos de modo general para llevar a cabo cualquier cesión.

Por otra parte, también es posible la cesión de dato de correo electrónico por medio de su publicación o publicidad, no ya a través de un canal electrónico, sino mediante su consulta a servicios de información telefónica. Al respecto, establece el apartado 4.2 de la Orden ministerial 711/2002, de 26 de Marzo, del ministerio de Ciencia y Tecnología:

> *Sin perjuicio de lo establecido en el punto primero de este apartado, y con la salvaguarda de la protección de los datos personales a la que se refiere el apartado 3º, mediante el servicio de consulta telefónica de números de abonado se podrá proporcionar información sobre otros recursos identificativos de abonados de servicios de telecomunicaciones disponibles al público, tales como direcciones de correo electrónico o nombres de dominio…*

La remisión al apartado 3º de esta Orden, implica que la inclusión de estas informaciones en estos servicios de información telefónica, exige el consentimiento inequívoco del abonado, mediante escrito del mismo dirigido al prestador del servicio o contestación fehaciente al requerimiento de éste último. Es

---

Europea por GAUTHRONET, SERGE y DROUARD, ÉTIENNE. *Comunicaciones comerciales no solicitadas y protección de datos.* (Enero de 2001). Pág. 8.

[207] No obstante, muchas de las cláusulas relativas a estas operaciones no están redactadas con la claridad deseable. Como ya hemos dicho en otras ocasiones, no se satisface el principio de finalidad, dado que se observa una gran vaguedad en los objetivos perseguidos por el cedente y el cesionario. Incluso en algunos casos se observan contradicciones, pues tras señalar que los datos recogidos no serán objeto de cesión, se solicita que para que no se produzca tal cesión debe comunicarse mediante correo electrónico a la página en cuestión. Tal es el caso de Amazon.com, según se afirma en un informe de EPIC (Electronic Privacy Information Center). EPIC. *Surfer beware: personal privacy and the Internet* (Junio, 1997). http://www.epic.org/ .

decir, se exige consentimiento expreso para poder proporcionar estas informaciones, solución que entendemos debe extrapolarse analógicamente a los demás medios de información existentes. Por cierto, que tal solución implica el reconocimiento de la dirección de correo electrónico como un dato de carácter personal.

Distintas de las anteriores son las captaciones de datos de carácter personal que se producen como consecuencia de las búsquedas o prospecciones en la red de dicha información por potentes herramientas destinadas al efecto, las cuales recogen toda la información que aparece en las páginas o espacios públicos. Generalmente, los foros de discusión y los chats, ya enunciados antes, son los principales ámbitos de los que se nutren tales buscadores. También recoge información en los diferentes listados de personas que aparecen en la red, de las páginas exclusivamente personales, entre otros sitios. Uno de los datos que de forma común se capta es el correo electrónico. La principal característica de estas operaciones es que han sido realizadas sin que el usuario ni el titular de la página web tengan conocimiento de la misma y, por supuesto, sin que medie consentimiento alguno. La segunda circunstancia que debemos tener en cuenta es la publicidad de los contenidos o sitios de los que se capta tal información. Tales hechos pueden ser contradictorios, en tanto que la publicación de los datos elimina la necesidad de consentimiento. La solución a esta cuestión requiere plantearse la finalidad de la captación y posterior utilización de esta información.

Si bien es cierto que cuando un usuario consiente a la publicación de determinada información, renuncia a la absoluta privacidad de la misma, sin embargo no se trata de una renuncia total en el sentido de que sus actos impliquen una aceptación total de los posibles usos que se pudieran hacer de aquélla. La publicación de un dato de carácter personal en la red no implica la total inaplicación del régimen jurídico de protección de datos. Como hemos dicho anteriormente, el principio de finalidad exige que los datos vayan a ser tratados de acuerdo con los fines para los que se recabaron, según se haya informado. Además, la captación debe legitimarse por la concurrencia del consentimiento, siquiera mediante el derecho de exclusión, de los usuarios.

Dudamos que, según que fines pudiere tener la cesión, los usuarios vayan a consentir cualquiera de éstas. El problema radica en la falta de conocimiento de que tales cesiones se han producido, por lo que difícilmente el sitio que recoge los datos puede informar y solicitar el consentimiento, dado que los datos se recaban porque son expuestos en la red para conocimiento general. Aún así, no es posible admitir cualquier posibilidad de uso. En este sentido, parece que estas formas de captación y, por lo tanto, su posterior uso para envío de correos, resultan contrarias a los principios fundamentales de la protección de datos de carácter personal, ya mencionados. Con arreglo a la LOPD y su Directiva de origen (95/46), tales prácticas deben ser reprimidas por su carácter ilícito.

En relación con estos métodos de recogida de información personal (y en general con todas las formas de obtención de direcciones de correo electrónico), uno de los problemas actualmente más debatidos es el relativo al *spam*. También denominado correo basura (*junk mail*, concepto este que, aunque no coincide plenamente con el spam y pudiere, por tanto, emplearse de forma incorrecta, es muy cercano al mismo) o buzonfia[208], se puede definir como *el envío masivo – y a veces repetido – de correos electrónicos no solicitados, generalmente de carácter comercial, dirigidos a personas con las que el remitente no ha tenido nunca contacto alguno que ha recogido la dirección electrónica de espacios públicos en Internet: foros de discusión, listas de distribución, anuarios, sitios web, etc*[209].

El spam ha generado, desde su aparición, grandes controversias en la comunidad de usuarios de Internet. El grado de sensibilidad frente al mismo es elevado, pues ocasiona una serie de inconvenientes y perjuicios de carácter tanto personal como económico. Efectivamente, los defectos que se achacan a esta forma de envío publicitario son: la recogida de la dirección de correo electrónico por quien remite los mensajes sin conocimiento ni consentimiento del usuario, el molesto *bombardeo* publicitario a que se ven sometidos los usuarios y la generación de un coste que, en la mayoría de los casos, dichos usuarios no asumirían voluntariamente. En efecto, las molestias son palpables, dado que el usuario tiene que invertir parte de su tiempo en abrir mensajes que ni ha solicitado ni seguramente son de su interés. Debemos tener en cuenta que la falta de indicación de la naturaleza del mensaje en su cabecera hace que, en la mayoría de los casos, se deban abrir los mismos sin conocer su contenido. A lo anterior debemos unir el hecho de que los usuarios deben descargar la memoria que ocupan los mensajes, sobre todo si se trata de correo web, dado que no puede ocupar más espacio del que le asigna en este caso el servidor de correo. Finalmente, la baja velocidad de la red provoca que la dedicación proporcionada a esta tarea sea desmesurada en relación con el fin.

Una de las principales quejas, tanto de usuarios como de los servidores de correo, es el elevado e innecesario coste que suponen las descargas de estos correos. Como ya sabemos, un usuario de correo electrónico que desee leer los mensajes debe conectar con el servidor para que aquéllos se descarguen a su ordenador (en el caso del correo web tal operación también se realiza, pero no supone descarga en el equipo cliente, sino visualización en la página en la que se encuentra el usuario). Ello supone un tiempo de conexión, que varía según la velocidad de la red en

---

[208] Término este empleado en la versión en castellano de varios informes y recomendaciones del Grupo de Trabajo del artículo 29 de la Directiva 95/46.

[209] Es la definición que de este fenómeno se recoge en CNIL. *Le publipostage électronique et la protection des données personnelles*. Pág. 1. Aunque como hemos visto, existen otras denominaciones, han triunfado la terminología inglesa, la cual no tiene una significado propio y concreto, sino que se trata de un término recogido de un guión de una película, en una de cuyas escenas se repetía esta palabra hasta la saciedad. De ahí su adopción para referirse a esta práctica.

ese momento[210]. También suponen un coste para los servidores de correo electrónico, que tienen que almacenar durante un período de tiempo dichos mensajes en sus equipos: han sido muchas las empresas dedicadas a esta actividad que han manifestado su malestar al respecto, algunas incluso han tratado de adoptar medidas técnicas[211].

Por el contrario, los beneficios para los remitentes de correos son palpables, dada la reducción de costes que supone la utilización de estos medios (el coste medio de un correo electrónico en E.E.U.U. es de 10 centavos, por los 50 centavos, como mínimo, que se deben pagar por un correo ordinario. En Europa las diferencias son similares[212]). Por otra parte, permite personalizar en gran medida los mensajes que se envían, a la vez que consigue que los usuarios conozcan el contenido de aquéllos, permitiendo así dar publicidad al anunciante, en mayor medida, que los banners o pancartas de publicidad que aparecen superpuestas en las páginas web. En definitiva, observamos que no existe una situación de equilibrio entre la posición de los usuarios y la que ostentan los remitentes de correo que utilizan como método el spam[213].

Ahora bien, además de los anteriores inconvenientes, que se encuadran dentro de un análisis económico del problema, el spam afecta también a la protección de los datos de carácter personal, en tanto que las direcciones de correo electrónico que se utilizan a tal efecto, se han podido recoger o ceder mediante prácticas que

---

[210] La CNIL calcula que el tiempo medio de descarga de los mensajes de 10 segundos. Nos parece, al menos respecto de las conexiones efectuadas en España, una estimación demasiado optimista. Además, hemos de pensar que los mensajes de publicidad suelen contener texto e imágenes, las cuales ocupan más memoria y, por tanto, tardan más en descargarse. Además, la mayoría de estos mensajes no van acompañados de la identificación del remitente, por lo que los usuarios no pueden decidir previamente sobre la conveniencia o no de descargarlos. CNIL. *Le publipostage électronique et la protection des données personnelles*. Pág. 6.

[211] A este respecto, la empresa estadounidense America Online obtuvo el reconocimiento judicial tendente a estas medidas, frente a la empresa Cyberpromotions, dedicada al envío de mensajes no solicitados. Entendió el tribunal que no se podía considerar al proveedor como un foro a través del cual se pudiera desarrollar la libertad de expresión. Con ello, la remitente no se podía amparar en la Primera enmienda. Citada en MUÑOZ MACHADO, SANTIAGO. *La regulación de la red*… Pág. 145.

[212] GAUTHRONET, SERGE y DROUARD, ÉTIENNE. *Comunicaciones comerciales no solicitadas*…. Pág. 2.

[213] Este desequilibrio es uno de los argumentos que el Grupo de Trabajo aporta para justificar la ilicitud de la captación de las direcciones de correo electrónicos desde los espacios públicos existentes en la red, en aplicación del artículo 7 f) de la Directiva 95/46, según el cual el tratamiento justifica, entre otras razones, *cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento… siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado*. GRUPO DE TRABAJO SOBRE PROTECCION DE DATOS DEL ARTÍCULO 29. *Dictamen 1/2000, sobre determinados aspectos de protección de datos del comercio electrónico* (3 de Febrero de 2000). 5007/00/ES/final.

suponen incumplimiento de la normativa sobre protección de datos. Pudieren existir argumentos que permitan soslayar este planteamiento, sin embargo ya adelantamos que, a nuestro parecer, la solución adecuada es la contraria.

Existe un sector de opinión que sostiene que el spam plantea una problemática que es propia de la práctica comercial. Desde este punto de vista, se afirma que la solución a las cuestiones generadas por aquél debería aportarse por la normativa propia de esta actividad. De esta forma, se trataría de adoptar un régimen jurídico que se encuadraría, para articular la defensa de los usuarios de Internet, dentro del más amplio Derecho de Consumo. Tal posición parece que coincide con el espíritu de algunas iniciativas legislativas sobre la materia. En efecto, la regulación del correo no solicitado se encuentra recogida, por primera vez, en la Directiva sobre protección de los consumidores en materia de contratos a distancia. El legislador español se ha planteado esta cuestión a la luz de la regulación de los servicios de la Sociedad de la información, conforme se deduce del texto de la Ley sobre la materia.

Desde otro punto de vista, algún autor sostiene que la protección a los usuarios respecto del spaming puede provenir de la regulación sobre publicidad. Así, se afirma que tales prácticas pueden constituir un supuesto de publicidad ilícita, la cual se define por el artículo 3 a) de la Ley de 11 de Noviembre de 1988, General de Publicidad, como

> *La publicidad que atente contra la dignidad de la persona o vulnere los derechos o valores reconocidos en la Constitución.*

Aunque en efecto la citada legislación de publicidad acoge una regulación del problema respetuosa con la índole estrictamente personal de esta cuestión, no ocurre lo mismo con las regulaciones anteriormente citadas. Sin negar que el spaming plantea interrogantes de naturaleza comercial, sin embargo se debe ir más allá. Existen, para ello, varios argumentos. En primer lugar, el carácter personal de la dirección de correo electrónico, como ya se ha dicho. Por otra parte, la publicidad del dato no excluye la aplicación del régimen de protección de datos, como también se dijo. Además, la realidad puede enfocarse y regularse desde distintas ópticas, de manera que aparezcan distintas normativas sobre un mismo problema, en función de cuáles sean los intereses objeto de las mismas. Resulta común que una misma cuestión se configure como zona secante de varias regulaciones, que abordan aquéllas desde distintas perspectivas.

Lo anterior se corrobora por la propia legislación comunitaria y su adaptación interna por los derechos nacionales. La Directiva 97/66, sobre protección de datos en el sector de las telecomunicaciones, regulaba en su artículo 12 las prospecciones realizadas mediante llamadas automáticas no solicitadas. Sin embargo, los preceptos de esta Directiva resultaban de difícil aplicación a las comunicaciones que se producen a través de Internet: por ello, debe sustituirse el concepto central de

llamada por el de comunicación, que engloba una realidad más amplia. En este sentido, parece acertada la regulación contenida en la Directiva 2002/58.

Sea cual sea la opción reguladora que se acoja, es necesario precisar el concepto de spam o de comunicación comercial no solicitada, en palabras de la legislación española. Se entiende por tales comunicaciones los mensajes que persiguen la promoción de bienes o servicios de quien desarrolla una actividad comercial, artesanal, industrial o profesional. Así, como recuerda Plaza Penades[214], quedan fuera del ámbito de esta definición los mensajes que permiten acceder a la actividad de la empresa, dominio, dirección de e-mail, entre otros. Es decir, parece que se establece una distinción, no exenta de ciertas dificultades, entre información y publicidad.

La principal característica del spam es la ausencia de voluntad alguna del usuario respecto de su recepción y su naturaleza comercial: son las dos notas que se reproducen de forma idéntica en las llamadas automáticas. Por esta razón, existe, desde hace algún tiempo, un claro interés por parte de la legislación sobre protección de datos en regular las comunicaciones no solicitadas. El Grupo de Trabajo aplaudía ya la decisión de los legisladores comunitarios, al afirmar que

> *…apoya la propuesta de dispensar al problema del correo electrónico no solicitado un tratamiento idéntico al de los sistemas de llamada automática sin intervención humana y los aparatos de fax. En todas estas situaciones, el abonado carece de interfaz humano y sufraga parte de los costes de la comunicación. El grado de violación de la intimidad son comparables en los tres casos*[215].

Sobre la base de la consideración del spam como un problema que afecta a la privacidad y la protección de los datos de carácter personal de los usuarios de Internet, es necesario determinar su régimen jurídico. Para ello, debemos acudir tanto al régimen general, recogido en la Directiva 95/46 y en la LOPD, como al sectorial de las telecomunicaciones, de la Directiva 2002/58 y la legislación española de adaptación (L.G.Tel. y R.S.U., ya estudiados anteriormente). Además, debemos partir del hecho de que tales correos son posibles como consecuencia de la recogida o las cesiones o comunicaciones de datos que previamente se han realizado a los remitentes.

---

214 PLAZA PENADES, JAVIER. *Los principales aspectos de la Ley de servicios de la sociedad de la información y comercio electrónico.* En *Contratación y comercio electrónico.* ORDUÑA MORENO, FRANCISCO JAVIER (Dirección), CAMPUZANO LAGUILLO, ANA BELEN y PLAZA PENADES, JAVIER. (Coordinación). Ed. Tirant lo Blanch. VALENCIA, 2003. Pág. 46 y ss.

215 GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas 12 de Julio de 2000* (2 de Noviembre de 2000). COM (2000) 385. 5042/00/ES/Final.

Si bien los diferentes estudios sobre la cuestión sólo consideran cesión la efectuada voluntariamente por el servidor de correo a un tercero, que remite los datos al mismo, sin embargo la captación por éste último de los datos publicados en la red implica, según la definición de cesión que recoge el artículo 3 de la LOPD (revelación de dichos datos a persona distinta del afectado), una cesión, siquiera con destinatario genérico, como ha sostenido la Agencia Española de Protección de Datos, según ya se ha visto. En este sentido, los requisitos exigidos deberían ser idénticos en uno y otro caso. No obstante, debemos tener en cuenta que la publicación implica una serie de posibilidades que el usuario debe tener en cuenta a la hora de autorizar, en su caso, aquélla.

El régimen jurídico de las cesiones que efectúan quienes reciben del usuario la dirección de correo a un tercero no difiere del general, que ya hemos mencionado anteriormente: información previa, lealtad y legitimidad del tratamiento y derecho de oposición. Respecto del consentimiento del usuario a los fines a los que se destinan los datos cedidos, la única referencia normativa que encontramos es el artículo 13.2 de la Directiva 2002/58, el cual regula la recepción de las comunicaciones por medios distintos a los mencionados en el párrafo 1º, de llamadas no solicitadas. En este caso, a diferencia del párrafo 1º, que exige el consentimiento previo del abonado para poder utilizar dichos medios, la Directiva permite la solución de ofrecer a los abonados el derecho de oposición de los abonados en el momento de recogida de las señas electrónicas (la Directiva 97/66, en su artículo 12.2, ofrecía la opción del consentimiento previo o del derecho de oposición). En el caso español, el artículo 68.2 del R.S.U. adoptaba ya esta solución. Aunque la regulación del spam no tiene que verse vinculada de forma obligatoria a lo dispuesto en este precepto, por el específico ámbito de esta Directiva, sin embargo no se puede negar que se trata de un precedente significativo. Además, en concordancia con la regulación española, la Directiva 97/7, de 20 de Mayo, sobre protección de consumidores en materia de contratos a distancia[216], establece en su artículo 10.2 que

> *Los Estados miembros velarán por que las técnicas de comunicación a distancia distintas de las mencionadas en el apartado 1* (sistemas de llamadas automáticas y fax)*, cuando permitan la comunicación individual, sólo puedan utilizarse a falta de oposición manifiesta del consumidor.*

Estas otras técnicas vienen recogidas en el Anexo de la Directiva, entre las que se menciona el correo electrónico. La regulación comunitaria más reciente sobre la materia se encuentra en la Directiva 2000/31, sobre comercio electrónico[217]. El artículo 7.2 de la misma establece que

---

[216] Documento 397L0007. Diario oficial núm. L 144 de 4-6-1997. Págs. 19-27.

[217] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de Junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre Comercio electrónico). Diario oficial nº L 178 de 17/7/2000. Págs. 1-16.

> *Sin perjuicio de lo dispuesto en las Directivas 97/7/CE* (contratos a distancia) *y 97/66/CE* (protección de datos en el sector de las telecomunicaciones)*, los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria ("opt-out") en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten.*

Como se puede observar, esta norma también aboga de forma expresa por la posibilidad de envío de correo no solicitado si no media la oposición del usuario: es decir, no prohíbe las comunicaciones comerciales no solicitadas, sino que exige que sean identificables de forma clara e inequívoca, en palabras de Pardo Leal[218]. Reseñamos estas afirmaciones porque la solución final, adoptada por la legislación interna, no ha sido la mencionada, como veremos a continuación. García Más entiende que no obstante la adopción por la Directiva del sistema *opt-out*, nada obsta a que la legislación interna abogue por la exigencia del consentimiento, como defendió la delegación española en los trabajos de elaboración del texto comunitario[219].

Por otra parte, el posible ahorro de molestias que implica el sistema *opt-out*, se ve compensado con la exigencia de consulta de las listas de exclusión, con lo que aquél pierde gran parte de su virtualidad. A este respecto, Vilches Trasierra recuerda que una de las críticas realizadas a la redacción del Proyecto de 18 de Enero de 2001, fue precisamente la obligación de los prestadores de servicios de consultar las listas de exclusión, a lo que se unía la falta de control del cumplimiento de dicha obligación[220].

Sin embargo, la LSSICE desecha la solución anterior. Dispone el artículo 21 de la misma:

> *Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.*

---

[218] PARDO LEAL, MARTA. *La Directiva 2000/31/CE sobre el Comercio electrónico: su aplicación en el ámbito del mercado interior.* Gaceta jurídica de la Unión europea y de la competencia, núm. 210. Noviembre-Diciembre de 2000. Pág. 48.

[219] GARCIA MAS, FRANCISCO JAVIER. *Comercio y firma electrónicos. Análisis jurídico de los servicios de la Sociedad de la información.* Ed. Lex nova. VALLADOLID, 2002. Pág. 173.

[220] VILCHES TRASIERRA, ANTONIO JOSE. *Aproximación a la Sociedad de la información: firma, comercio y banca electrónica.* Centro de estudios registrales. MADRID, 2002. Pág. 130.

Previamente, el artículo 20.1 exige a los remitentes que identifiquen, en el espacio reservado al asunto, el carácter publicitario del mensaje con la palabra "publicidad", de conformidad con las exigencias de información establecidas en el artículo 6 de la Directiva 2000/31. Esta obligación permite, por tanto, a los usuarios, evitar la descarga de los mensajes desde el servidor a sus equipos y proporcionar, así, una posición equivalente a la que tienen aquéllos respecto de la publicidad envidada por correo ordinario[221]. No obstante el avance que puede suponer lo anterior, aunque se minimizan los problemas de costes para los usuarios, no ocurre lo mismo respecto de las exigencias de ampliación de equipos técnicos para los servidores de correo.

Así, la legislación aboga claramente por la exigencia de consentimiento expreso, lo cual supera con mucho, la solución de la posibilidad de oposición de los usuarios que acoge la normativa comunitaria, a la vez que se sobrepone a las grandes presiones sufridas por el legislador comunitario[222]. Esta disfunción normativa parece haberse resuelto con la aparición de la Directiva 2002/58. Por una parte, señala su artículo 13.1:

> *Sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.*

Es decir, se exige en los supuestos de comunicación automática no solicitada el consentimiento previo. Además, no se debe perder de vista el ámbito objetivo de esta exigencia, pues *sensu* contrario el consentimiento expreso no se exige cuando las comunicaciones no se efectúan a través de los medios mencionados en el precepto anterior, como por ejemplo ocurre en el caso de los mensajes SMS enviados mediante el uso de un teléfono móvil, según recuerda Cimas[223]. A continuación, el párrafo 2º del mismo artículo dispone lo siguiente:

> *2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de las venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta*

---

221 MARQUEZ LOBILLO, PATRICIA. *Op. cit.* Pág. 345.

222 Al respecto, CIMAS, MARTA. *Protección de datos y telecomunicaciones. Regulación actual y exigencias de la nueva Directiva*… Pág. 304.

223 CIMAS, MARTA. *Protección de datos y telecomunicaciones. Regulación actual y exigencias de la nueva Directiva*… Pág. 305.

claridad a sus clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.

Como se afirma en el Considerando 41, es razonable admitir el envío de mensajes de correo electrónico en el contexto de una previa relación con el cliente (de ahí el subrayado). Entendemos que puede existir un exceso de *razonabilidad* en los términos de la Directiva, pues en muchos casos, los clientes no desearán mantener contacto alguno continuo con el oferente: si así lo desean, ya contactarán los primeros con los segundos. En cualquier caso, como afirma Muñoz Machado, no se prohíbe el spaming, sino que se posibilita el control por los afectados[224], lo cual no parece acorde con la solución taxativa adoptada por la LSSICE.

A juicio de algunos autores, la solución adoptada por la LSSICE resulta excesiva, pues se entiende que se trata de una práctica común en el mercado real, cuya prohibición no se justifica por el medio empleado. Prueba de ello, según los autores, es la postura permisiva de la legislación comunitaria[225]. No obstante, creemos que tales afirmaciones se hacen desde una perspectiva puramente contractual del problema, sin tener en cuenta la problemática añadida de la protección de datos. En realidad, se trata de una postura adecuada a los fines que de modo general se propone alcanzar la Directiva. En la Exposición de Motivos de la Propuesta de esta Directiva se afirmaba que el objetivo principal de la reforma es la conveniencia de adoptar un régimen neutro desde el punto de vista tecnológico, lo que exige que los usuarios de estos medios deben tener el mismo nivel de protección cualquiera que sea la naturaleza o características de la tecnología utilizada. Así, la inclusión del correo electrónico dentro del párrafo 1º del artículo 13 está plenamente justificada. No obstante, pudiera plantearse el sentido el párrafo segundo, dado que permite un nivel de protección menor, pues en la práctica muchos usuarios no ejercerán su derecho de oponerse.

En cualquier caso, ¿cómo se puede congraciar la aparente contradicción entre las normativas comunitaria e interna?. Debe observarse que los criterios de distinción adoptado en el artículo 13, para establecer la exigencia de consentimiento previo o el derecho de oposición, es la falta de solicitud en el primer caso y la existencia de una previa relación entre las partes, en el segundo. En definitiva, se adopta una solución diversa según haya habido o no relación previa con el cliente. La Directiva debe partir de la concurrencia de una voluntad favorable, pues en caso contrario no se justifica la posibilidad de oponerse. Como ya hemos señalado, pudiere resultar excesivo deducir de dicha relación, la intención de mantener de forma continuada comunicación con los oferentes.

---

224 MUÑOZ MACHADO, SANTIAGO. *La regulación de la red…* Pág. 147.

225 MARTINEZ MATESANZ, CARMEN y RUIZ MUÑOZ, MIGUEL. *Algunos aspectos jurídico-privados del Proyecto de Ley de SSI y de Comercio electrónico de 8 de Febrero de 2002*. Revista de la contratación electrónica, núm. 27. Mayo de 2002. Pág. 43.

La Directiva 2002/58 también justifica esta novedad por la lógica necesidad de armonizar las legislaciones europeas para eliminar una situación paradójica. Algunos países han prohibido el spam sin consentimiento previo (Alemania, Austria, Italia, Finlandia y Dinamarca), lo que se materializa en la inclusión del usuario en una lista al efecto, mientras que en otros se adoptaba la solución contraria, que permite el envío de aquél a todos los usuarios que no hayan sido incluidos en una lista de exclusión, a lo que se une la circunstancia de que las direcciones de correo electrónico no suelen expresar la ubicación del destinatario en uno u otro Estado. Así, se podía dar el caso de que remitentes de spam de un país perteneciente al primer grupo pudiera mandar correos a ciudadanos de países del segundo y no a sus propios conciudadanos.

En cualquier caso, la novedad que puede implicar, en su caso, la Directiva 2002/58 obliga a los legisladores a un replanteamiento de estas cuestiones en los Estados miembros, dada la contradicción normativa existente.

En realidad, la existencia de disparidades entre las regulaciones antes citadas obedece a las diversas visiones o perspectivas desde la que, a su vez, se puede analizar el problema del spam. Como ya hemos dicho, en el tratamiento de este problema deben observarse distintos intereses: el puramente personal de la protección de los datos de carácter personal, el económico de los costes que el spam implica para los usuarios y los servidores de correo, las molestias acarreadas a los primeros. Si bien la legislación existente parece indicar que el interés protegible es de naturaleza comercial o económica, sin embargo la aparición de la Directiva 2002/58 vuelve a reconducir el análisis al ámbito de la protección de derechos fundamentales de los individuos, al menos según se deduce del título de la misma. Es decir, no solamente se trata de proteger la posición de los usuarios en tanto que consumidores, sino que además es necesario tener presente las afecciones a la privacidad de los mismos, en tanto que personas sin más, desprovistos de su carácter de adquirentes de bienes y servicios.

En un primer momento, no éramos muy optimistas respecto de la verdadera preocupación que habría movido al legislador a interesarse por estas cuestiones. En realidad, la ubicación de esta problemática en regulaciones relativas a la actividad comercial (ventas a distancia, comercio electrónico) parece indicar que el objetivo en la mente de aquel no es, principalmente, resolver problemas relativos a la protección de datos de carácter personal. Por otra parte, la adopción de una solución distinta a la que recogía la Directiva 97/66, sobre protección de datos en el sector de las telecomunicaciones, no obstante estar de acuerdo con ella, nos induce a pensar que la postura del legislador venía determinada por una intención que no es la citada protección de los datos, pues en caso contrario no se hubiese producido tal modificación.

En este sentido, no podemos olvidar la presión ejercida por los diferentes sectores económicos afectados, así como por la propia opinión pública. Las tendencias provenientes de E.E.U.U., más avanzados en esta materia por haber sufrido antes los perjuicios derivados de estas prácticas, manifiestan un reforzamiento del control de los usuarios en la recepción de los correos no solicitados. No obstante, las verdaderas razones obedecen a las soluciones adoptadas por las compañías de marketing, que han comprobado que la solicitud previa del consentimiento de los usuarios garantiza la mayor calidad y veracidad de los datos proporcionados y una postura más receptiva de los mismos. Por otra parte, la postura del sector en el ámbito europeo no es tan avanzada como la norteamericana: los operadores proponen el mantenimiento de la exigencia del consentimiento tácito (*opt-out*), siquiera reforzado con mayores garantías.

En línea con lo anterior, un amplio sector doctrinal también considera que las razones de carácter económico son la verdadera motivación de la solución adoptada por la regulación sobre comercio electrónico. Sostiene Hernández Jiménez-Casquet[226] que tal conclusión se deduce del hecho de que la forma expresa de consentir no se exige respecto de otras formas de comunicación, como el correo ordinario o el teléfono. Fundamentalmente, la exigencia del consentimiento expreso pretende conseguir un ahorro de costes al destinatario de los mensajes, más bien, pretende evitar un gasto.

Sea como fuere, debemos aplaudir la solución adoptada por el legislador español. En la LSSICE no sólo se adopta una solución respetuosa con la protección de los datos de los usuarios, sino que además se adopta una medida tendente a evitar las dilaciones ocasionadas por la aparición de un correo publicitario no solicitado[227]. Concretamente, se impone la mención inicial del carácter comercial del mensaje. No obstante lo adecuado de tal deber, sin embargo el mismo no satisface plenamente las pretensiones de los usuarios desde un punto de vista económico, pues tal mención solamente se conoce cuando el mensaje ya ha llegado a nuestro equipo, de forma que no se puede evitar el coste económico de su descarga desde el servidor. Para lograr tal objetivo, es conveniente el empleo de herramientas o servicios informáticos que ejercen una función de filtro.

---

[226] HERNANDEZ JIMENEZ-CASQUET, FERNANDO. *El marco jurídico del comercio y la contratación electrónicos*. En *Principios de derecho de Internet*. Director: Pablo García Mexía. Ed. Tirant lo Blanch. VALENCIA, 2002. Pág. 364. La misma razón económica justifica esta solución, a juicio de Plaza Penades. PLAZA PENADES, JAVIER. *Los principales aspectos de la Ley de servicios de la sociedad de la información y comercio electrónico*… Pág. 46.

[227] La exigencia de consentimiento previo en los casos de correos no solicitados debería, como sostiene Loza Corera, aplicarse igualmente a los supuestos de comunicaciones no solicitadas por otros medios de comunicación, como las llamadas no solicitadas, aparatos de rellamada y otros regulados por la normativa de telecomunicaciones. En efecto, así creemos que debe ser, puesto que no observamos diferencias apreciables respecto de la protección de los usuarios en ambos casos. LOZA CORERA, MARIA. *Nueva legislación europea en materia de*… Pág. 4.

En otro orden de cosas y desde la óptica de la protección de datos, las listas de inclusión o la exigencia del consentimiento previo son más respetuosas, no sólo por la concurrencia de la voluntad del usuario, sino porque dichos listados no son susceptibles de cesión remunerada, a diferencia de las listas de exclusión. Esta última posibilidad pudiere resultar injusta por su carácter general, dado que la voluntad de exclusión afectaría a todos los potenciales remitentes de mensajes, sin admitir la posibilidad de voluntades distintas de los usuarios, según quienes sean aquéllos[228]. Como se observa claramente, se consigue proteger la privacidad de los usuarios mediante la consecución de fines propiamente empresariales, pues las empresas del sector de marketing han observado los beneficios que implica la concurrencia del consentimiento de los usuarios, no ya para éstos, sino para *la satisfacción de los fines propios de la prospección comercial*. De cualquier forma, aplaudimos la adopción de este tipo de soluciones, pero dudamos de las verdaderas razones que subyacen en este caso. No obstante, no podemos dejar de reconocer los apoyos que las listas de exclusión reciben de algún sector doctrinal, más bien preocupado por la dimensión comercial o empresarial de este problema[229].

Tampoco podemos olvidar la postura contraria que muchos prestadores de servicios de Internet y, específicamente, de correo electrónico, han mostrado frente al spam, tanto por los motivos técnicos ya apuntados como por la postura remisa que perciben en sus usuarios, sobre todo en el territorio europeo, lo que ha provocado el cambio de percepción del problema en las prácticas de marketing. Igualmente, se observa una postura de rechazo al spam en la legislación de diferentes Estados de E.E.U.U., que imponen multas importantes a las empresas que emplean estos métodos, pues generalmente no son de gran tamaño. Tal normativa ha producido un efecto disuasorio.

Finalmente, respecto del consentimiento para ceder estos datos, en la práctica de las compañías que recaban datos o los obtienen por cesión es normal que los mismos se vuelvan a ceder a su vez por el cesionario inicial. La necesidad de consentimiento específico plantea dudas respecto de la necesidad de que el mismo concurra en cada una de aquéllas.

---

228 Los beneficios derivados de esta opción son múltiples, como se puede observar. En este sentido, Informe elaborado para la Comisión Europea por GAUTHRONET, SERGE y DROUARD, ÉTIENNE. *Comunicaciones comerciales no solicitadas*…

229 Para Miquel Rodríguez, el sistema *opt-out* resulta proporcionado a los intereses en juego, a la vez que elimina los problemas de control en origen de la publicidad. MIQUEL RODRIGUEZ, JORGE. *Problemática jurídica de la publicidad en Internet.* En *Comercio electrónico y protección de los consumidores.* Coor. BOTANA GARCIA, GEMA. La Ley. MADRID, 2001. Pág. 255.

El Consejo de Europa[230] ha sostenido que, por razones de agilidad, es admisible un consentimiento inicial, con independencia del número de cesiones que se vayan a realizar (parágrafo 3.1). Lo cierto es que, aunque en el momento inicial no se conozca el posible número de cesiones que se vayan a realizar, sin embargo el cumplimiento del principio de finalidad no permite pensar que tal posibilidad se encuentre limitada a aquéllas que satisfagan los objetivos para los que se obtuvo el consentimiento. Para garantizar el cumplimiento de los requisitos necesarios para las cesiones y la determinación de las responsabilidades que se deban depurar, el Consejo de Europa recomienda que estas cesiones se articulen a través de contratos celebrados entre cedente y cesionario (parágrafo 3.2), evitando la generalidad de las normas o la ambigüedad de los códigos de conducta, que, por otra parte, no pasan de constituir un deber ético.

[230] CONSEJO DE EUROPA. *Recomendación Nº R (85) 20 del Comité de Ministros de los Estados miembros, relativa a los datos de carácter personal utilizados con fines de marketing directo.*

ABREVIATURAS.

ADSL: Asymmetric digital subscriber line.
APD: Agencia española de protección de datos.
APDCM: Agencia de protección de datos de la Comunidad de Madrid.
ATA: Anti-terrorism act.
BOCM: boletín oficial de la Comunidad de Madrid.
CNIL: Commission nationel de la l´informatique et des libertés.
DNS: Domaine name server.
EPIC: Electronic privacy information center.
FAPSI (en ruso): Agencia federal de comunicaciones e información del Gobierno.
FBI: Federal bureau of investigation.
FTP: Files tranfer protocol.
GCHQ: Goverment communications headquarter.
HTML: Hypertext markup language.
HTTP: Hypertext tranfer protocol.
LGTel: Ley general de telecomunicaciones.
LOPD: Ley Orgánica de protección de datos de carácter personal.
LOPJ: Ley Orgánica del Poder judicial.
LORTAD: Ley Orgánica reguladora del tratamiento automatizado de datos de carácter personal.
LSSICE: Ley de servicios de la sociedad de la información y del comercio electrónico.
NSA: National security agency.
POP: Post office protocol.
RSU: Reglamento de desarrollo del Título III de la LGTel.
SET: Secure electronical transaction.
SMTP: Simplemail tranfer protocol.
SSL: Secure socket layer
TCP/IP: Transfer control protocol/Internet protocol.
TEDH: Tribunal europeo de derechos humanos.
UKUSA: United Kindom-United States of America.
URL: universal resource locator.

BIBLIOGRAFIA.

ACED FELEZ, EMILIO. *Transacciones electrónicas en Internet.* Jornadas sobre Protección de la Privacidad, Telecomunicaciones e Internet. Pamplona, 2000.

ADAM COHEN. *Spies among us.* Time Europe. July 31, 2000. Vol. 156, núm. 5.

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Memoria de 1997 de la Agencia Española de Protección de Datos.

Memoria del año 1999.

Memoria del año 2000.

Recomendaciones a usuarios de Internet. MADRID, 1997. Memoria de 1997, Anexo IV.

Informes de la Agencia española de Protección de datos. www.agpd.es

ANCOS FRANCO, HELENA. *El tratamiento automatizado de los datos personales en el ámbito de las telecomunicaciones. Comentario a la Consulta 1/99 de la Fiscalía General del Estado.* LA LEY. Diario núm. 4812 de 7 de Junio de 1999.

ANTHONY GIDDENS Y WILL HUTTON, eds. *En el límite. La vida en el Capitalismo global.* Tusquets Editores, S.A. 2001, BARCELONA.

APARICIO SALOM, JAVIER. *Estudio sobre la Ley Orgánica de Protección de datos de carácter personal.*

ASIS ROIG, AGUSTIN E. *Protección de datos y derecho de las telecomunicaciones.* En *Régimen jurídico de Internet.* Colección derecho de las telecomunicaciones (Coord. CREMADES, JAVIER; FERNANDEZ-ORDOÑEZ, MIGUEL ANGEL; ILLESCAS ORTIZ, RAFAEL). Ed. La Ley. MADRID, 2002.

ASPAS ASPAS, JOSE MANUEL. *Las guías de servicios de telecomunicaciones y la protección de datos.* La Ley, núm. 1. 2000.

BELDA PEREZ-PEDRERO, ENRIQUE. *El derecho al secreto de las comunicaciones: algunos sobre su protección en las relaciones por correo electrónico. III Jornadas sobre Informática y Sociedad.* Instituto de Informática Jurídica. Facultad de Derecho. Universidad Pontificia de Comillas. 2001, Madrid.

BENSOUSSAN, ALAIN. *Internet. Aspects juridiques.* Ed. Hermès. PARIS, 1998.

BOTANA GARCIA, GEMA ALEJANDRA. *Noción de comercio electrónico.* En *Comercio electrónico y protección de los consumidores.* Coord. BOTANA GARCIA, GEMA ALEJANDRA. Ed. La Ley. MADRID, 2001. Pág. 57. También MARTINEZ NADAL, APOLONIA. *La protección del consumidor en la Propuesta de Directiva sobre determinados aspectos del comercio electrónico.* Cuadernos de derecho y comercio, núm. 29. 1999.

CARRASCO PERERA, ANGEL, MENDOZA LOSANA, ANA I. e IGARTUA ARREGUI, FERNANDO. *Comentarios a la Ley general de telecomunicaciones.* ARPON DE MENDIVIL ALDAMA, ALMUDENA y CARRASCO PERERA, ANGEL (Directores). Ed. Aranzadi. PAMPLONA, 1999.

CASTRO REY, JOSE LUIS. *Internet y la protección de datos de carácter personal en España.* Agencia de protección de datos, 1996.

CAVANILLAS MUGICA, SANTIAGO. *Telecomunicaciones y protección de la intimidad personal en el seno del grupo doméstico.* XII Encuentros sobre Informática y derecho, 1998-1999. Universidad Pontificia de Comillas. Ed. Aranzadi. MADRID, 1999.

CERVERA NAVAS, LEONARDO. *Comentarios a la Propuesta de reforma de la Directiva 97/66 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.* Jornadas sobre Protección de la Privacidad, Telecomunicaciones e Internet. Pamplona, 2000.

CIMAS, MARTA. *Protección de datos y telecomunicaciones. Regulación actual y exigencias de la nueva Directiva.* En *la nueva regulación de las telecomunicaciones, la televisión e Internet.* VILLAR URIBARRI, JOSE MANUEL (Director). Ed. Thomson-Aranzadi. MADRID, 2003.

CNIL. *Le publipostage électronique et la protection des données personnelles.* Se puede encontrar en http://www.cnil.fr/ .

COMISION EUROPEA. *Libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación (COM (97) Versión 3).*

CONSEJO DE EUROPA. *Recomendación Nº R (85) 20 del Comité de Ministros de los Estados miembros, relativa a los datos de carácter personal utilizados con fines de marketing directo.*

Recomendación nº R(99)5 del Comité de Ministros de los Estados miembros sobre la protección de la Intimidad en Internet, para la protección de las personas respecto a la recogida y tratamiento de datos personales en las autopistas de la información

CORRIPIO GIL-DELGADO, MARIA DE LOS REYES. *La protección de los datos personales en Internet.* Boletín del Ministerio de Justicia. Año LV. 15 de Septiembre de 2001.

CORRIPIO GIL-DELGADO, MARIA DE LOS REYES y MARROIG POL, LORENZO. *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones.* Agencia de protección de datos. MADRID, 2001.

Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet. Agencia de Protección de Datos. Premio protección de datos personales, IV edición. 2000, MADRID.

CREMADES, JAVIER y RODRIGUEZ-ARANA, JAIME. *Comentarios a la Ley General de Telecomunicaciones (aprobada por Ley 32/2003, de 3 de Noviembre).* Colección derecho de las telecomunicaciones. La Ley. MADRID, 2004. Pág. 532.

EPIC (Electronic Privacy Information Center). EPIC. *Surfer beware: personal privacy and the Internet* (Junio, 1997). http://www.epic.org/ .

FERNANDEZ ESTEBAN, MARIA LUISA. *Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las comunicaciones entre particulares, en especial en el ámbito de la empresa.* Aranzadi Civil, núm. 3. Mayo de 2000.

GARCIA MAS, FRANCISCO JAVIER. *Comercio y firma electrónicos. Análisis jurídico de los servicios de la Sociedad de la información.* Ed. Lex nova. VALLADOLID, 2002.

GARRIGUES DIAZ-CAÑABATE, JOAQUIN. *Tratado de derecho mercantil. Tomo I, vol. 3º.* Revista de derecho mercantil. MADRID, 1947-1964.

GAUTHRONET, SERGE y NATHAN, FREDERIC. *Les services en ligne et la protection des données et de la vie privée. Etude pour la Commission de Communautés Européennes (DG XV).* Págs. 91 y ss. Este trabajo se puede encontrar en http://www.europa.eu.int/.

GEORGE SOROS. *La crisis del Capitalismo global. La Sociedad abierta en peligro.* Ed. Debate. 1999, MADRID.

GRUPO DE PROTECCION DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES. *Recomendación 3/97, sobre Anonimato en Internet* (3 de Diciembre de 1997). XV D/5022/97 ES final.

Resolución 1/99, sobre tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware (23 de febrero de 1999).

Recomendación 3/99, sobre la conservación de los datos sobre tráfico por los proveedores de servicio de Internet a efectos de cumplimiento de la legislación. 7 de Septiembre de 1999.

Recomendación del Grupo de Trabajo del artículo 29 sobre determinación de los requisitos mínimos para la recogida en línea de los datos personales en la Unión Europea. 17 de Mayo de 2001.

Dictamen 1/2003, sobre almacenamiento de los datos de tráfico a efectos de facturación. 29 de Enero de 2003.

Dictamen 5/2002, sobre la Declaración de los Comisarios europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de Septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones.

Dictamen 1/2000, sobre determinados aspectos de protección de datos del comercio electrónico (3 de Febrero de 2000).

Dictamen 5/2000, adoptado el 13 de Julio, sobre el uso de guías telefónicas públicas para servicios de búsqueda inversa o multicriterio (Guías inversas).

Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas 12 de Julio de 2000 (2 de Noviembre de 2000).

Documento de Trabajo sobre servicios de autenticación en línea. 29 de Enero de 2003.

Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE. 30 de Mayo de 2002.

Documento de trabajo: tratamiento de datos personales en Internet (23 de Febrero de 1999). 5013/99/ES/final. También se encuentra en la página *http://www.europa.eu.int/*.

Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea (Documento de trabajo del Grupo de trabajo sobre

protección de datos del artículo 29). 21 de Noviembre de 2000. También en *http://www.europa.eu.int/*.

HEREDERO HIGUERAS, MANUEL. *La Directiva comunitaria de protección de datos de carácter personal*. Ed. Aranzadi. PAMPLONA, 1997.

La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Comentario y textos. Ed. Tecnos. MADRID, 1996.

HERNANDEZ JIMENEZ-CASQUET, FERNANDO. *El marco jurídico del comercio y la contratación electrónicos*. En *Principios de derecho de Internet*. Director: Pablo García Mexía. Ed. Tirant lo Blanch. VALENCIA, 2002.

ILLESCAS ORTIZ, RAFAEL. *Claroscuro con patitos: de nuevo sobre la legislación proyectada en materia de contratación electrónica*. Revista de contratación electrónica, núm. 27. Mayo de 2002.

LLANEZA GONZALEZ, PALOMA. *Internet y comunicaciones digitales*. Ed. Bosch. BARCELONA, 2000.

LOZA CORERA, MARIA. *Nueva legislación europea de protección de datos*. Diario la Ley, núm. 5549. Año XXIII. 22 de Mayo de 2002.

MADRID PARRA, AGUSTIN. *Contratación electrónica*. En *Estudios jurídicos en homenaje al Profesor Aurelio Menéndez*. Tomo III. Ed. Civitas. MADRID, 1996.

MANTECA VALDELANDE, VICTOR. *El proyecto de Ley de Internet y Comercio electrónico*. Diario La Ley, núm. 5508. 22 de Marzo de 2002.

MARQUEZ LOBILLO, PATRICIA. *Empresarios y profesionales en la sociedad de la información*. Cuadernos Mercantiles. FERANDEZ RUIZ, JOSE LUIS (Dirección). Ed. EDERSA. MADRID, 2004.

MARTIN MORALES, RICARDO. *El régimen constitucional del secreto de las comunicaciones*. Ed. Civitas. MADRID, 1995.

MARTINEZ MATESANZ, CARMEN y RUIZ MUÑOZ, MIGUEL. *Algunos aspectos jurídico-privados del Proyecto de Ley de SSI y de Comercio electrónico de 8 de Febrero de 2002*. Revista de la contratación electrónica, núm. 27. Mayo de 2002.

MARTIN-RETORTILLO BAQUER, LORENZO. *Comentarios a la Ley General de Telecomunicaciones (artículo 50). Coord. Eduardo García de Enterría y Tomás de la Quadra-Salcedo*. Ed. Civitas. Madrid, 1999.

MESSIA DE LA CERDA BALLESTROS, JESUS ALBERTO. *Cesión de datos, fusión y escisión de sociedades. Los grupos de empresas.* Revista datospersonales.org (revista digital de la Agencia de Protección de Datos de la Comunidad de Madrid). Nº 4, de 16 de Septiembre de 2003.

MIGUEL ASENSIO, PEDRO A. DE. *Derecho privado de Internet.* Ed. Civitas. MADRID, 2000.

MIRALLES MIRAVET, SERGIO y BACHES OPI, SERGIO. *La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos.* Revista de Derecho de Derecho Privado. Mayo de 2001.

MUNAR BERNAT, PEDRO A. *Protección de datos en el comercio electrónico.* En *Comercio electrónico y protección de los consumidores.* Coord. BOTANA GARCIA, GEMA ALEJANDRA. Ed. La Ley. MADRID, 2001.

MUÑOZ MACHADO, SANTIAGO. *La regulación de la red. Poder y Derecho en Internet.* Ed. Taurus. MADRID, 2000.

PARDO LEAL, MARTA. *La Directiva 2000/31/CE sobre el Comercio electrónico: su aplicación en el ámbito del mercado interior.* Gaceta jurídica de la Unión europea y de la competencia, núm. 210. Noviembre-Diciembre de 2000.

PARLAMENTO EUROPEO. COMISION TEMPORAL SOBRE EL SISTEMA DE INTERCEPTACION ECHELON. *Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y electrónicas (sistema de interceptación ECHELON).* Ponente: Gerhard Schmidt. 11 de Julio de 2001. FINAL A5-0264/2001 PARTE 1.

PINET, MARCEL. *Datos públicos o datos a los que puede acceder el público y protección de datos. XX Conferencia de protección de datos.* Agencia de Protección de Datos, 1998.

PLAZA PENADES, JAVIER. *Los principales aspectos de la Ley de servicios de la sociedad de la información y comercio electrónico.* En *Contratación y comercio electrónico.* ORDUÑA MORENO, FRANCISCO JAVIER (Dirección), CAMPUZANO LAGUILLO, ANA BELEN y PLAZA PENADES, JAVIER. (Coordinación). Ed. Tirant lo Blanch. VALENCIA, 2003.

RAMOS SUAREZ, FERNANDO. *¿Es legal el uso de las cookies?.* REDI (Revista electrónica de Derecho Informático). http//:v2.vlex.com/global/redi.

RAYNOUARD, ARNAUD. *La formation du contract électronique.* En *Le contract électronique.* Travaux de l´Association Henri Capitant. Journées nacionales, Tomo V. Toulouse, 2000. Ed. Panteón-Assas. PARIS, 2002.

RIBAS ALEJANDRO, JAVIER. *Riesgos legales de Internet. Especial referencia a la protección de datos personales.* En *Derecho de Internet. Contratación electrónica y firma digital.* Coord. MATEU DE ROS, RAFAEL y CENDOYA MENDEZ DE VIGO, JUAN MANUEL. Ed. Aranzadi. PAMPLONA, 2000.

Comercio electrónico en Internet. En *Problemática jurídica en torno al fenómeno de Internet* (Director. JUAN JOSE MARTIN-CASALLO LOPEZ). Cuadernos de Derecho Judicial. Consejo General del Poder Judicial. MADRID, 2000.

Aspectos jurídicos del uso de las cookies. http://www.onnet.es/.

ROCA JUNYENT, MIGUEL y TORRALBA MENDIOLA, ELISA. *Derecho a la intimidad: el secreto de las comunicaciones e Internet.* En *Régimen jurídico de Internet.* Colección Derecho de las telecomunicaciones (Coord. CREMADES, JAVIER; FERNANDEZ-ORDONEZ, MIGUEL ANGEL; ILLESCAS, RAFAEL). Ed. La Ley. MADRID, 2002.

RUIZ MIGUEL, CARLOS. *Protección de datos personales y comercio electrónico.* En *Comercio electrónico en Internet.* GOMEZ SEGADE, JOSE ANTONIO, FERNANDEZ-ALBOR BALTAR, ANGEL y TATO PLAZA, ANXO (coords.) Ed. Marcial Pons. MADRID, 2001.

SANCHEZ CALERO, FERNANDO. *Instituciones de Derecho Mercantil. Vol. I.* Ed. MCGraw Hill. Madrid, 2000.

SENADO. *Acuerdo del Pleno del Senado por el que se aprueba el Informe de la Comisión especial sobre redes informáticas.* Págs. 45 y 46. Boletín Oficial de las Cortes Generales. Senado. VI Legislatura. Serie I: Boletín General de 27 de Diciembre de 1999. Núm. 812. Este documento se puede encontrar en http://www.senado.es/.

URIA, RODRIGO. *Derecho Mercantil.* Ed. Marcial Pons. MADRID, 1998.

VATTIER FUENZALIDA, CARLOS. *Responsabilidad contractual y extracontactual en el comercio electrónico.* En *Régimen jurídico de Internet.* CREMADES, JAVIER; FERNANDEZ-ORDOÑEZ, MIGUEL ANGEL; ILLESCAS, RAFAEL (Coordinadores). Ed. La Ley. MADRID, 2002.

VILCHES TRASIERRA, ANTONIO JOSE. *Aproximación a la Sociedad de la información: firma, comercio y banca electrónica.* Centro de estudios registrales. MADRID, 2002.

www.assemblee-nationale.fr/2/2textes-a.html .

www.europa.eu.int.

www.silicon.com/a38414.