PROTECCIÓN DE LOS DATOS PERSONALES EN LAS COMUNICACIONES ELECTRÓNICAS: ESPECIAL REFERENCIA A LA LEY 25/2007, SOBRE CONSERVACIÓN DE DATOS

JOSÉ IGNACIO CUBERO MARCOS
UNAI ABERASTURI GORRIÑO

1. INTRODUCCIÓN

En los primeros pasos liberalizadores del sector de las telecomunicaciones las Directivas comunitarias contemplaron la necesidad de restringir la libre prestación de servicios en los casos en que fuera necesario para preservar los datos personales. Este límite se denominaba tradicionalmente un «requisito esencial» para la provisión del servicio. En otras palabras, en caso de que las redes de telecomunicaciones no ofrecieran las suficientes garantías para la protección y tutela de los datos personales, las autoridades internas podían fijar trabas para el ejercicio y desarrollo de la prestación del servicio.

Las citadas medidas tenían por objeto no sólo prevenir las posibles violaciones a la intimidad, sino también crear instrumentos suficientes para evitar que las innovaciones tecnológicas en el sector se convirtieran, en último término, en una forma más sutil de control social sobre los ciudadanos. Tanto la doc-

trina (1) como la jurisprudencia (2) han puesto de manifiesto los nuevos retos que plantea la revolución de las que se han venido en llamar Tecnologías de la Información y Comunicación con respecto al derecho de los ciudadanos a controlar sus datos de carácter personal. Hoy día constituye un argumento común que la ya prácticamente consolidada Sociedad de la Información plantea nuevas formas de amenaza para la intimidad y el derecho a la protección de los datos personales (3). La ampliación de la memoria de los ordenadores, la rapidez con la que fluye la información a través de la red y la diversidad de operadores que gestionan los datos de las comunicaciones se muestran como factores que impiden un efectivo control por parte del ciudadano de toda la información que discurre a través de la red (4).

Piénsese que una sola llamada, un único mensaje de correo electrónico, ya contiene información que afecta a la vida privada de los ciudadanos que inician las comunicaciones por estos medios. Por ejemplo, el lugar desde donde se ha llamado (localización), quién ha iniciado la comunicación y quién la ha recibido (identificación) y la fecha y hora de la transmisión de las señales. Cada llamada realizada o mensaje de correo electrónico enviado portan el número telefónico de quien la inicia o recibe o, en el caso de los correos electrónicos, la dirección de los que se comunican. En este punto cabe plantear numerosas cuestiones, como cuál es el período de tiempo máximo que los operadores pueden retener todos los datos relativos a números de teléfono o direcciones, qué operador puede tratarlos, gestionarlos o conservarlos y, lo que es más importante, en qué medida el usuario del servicio puede controlar la información de que dispone la compañía que le provee el servicio.

La Unión Europea, en plena cruzada contra el terrorismo a escala interna o internacional, y con motivo de los cruentos acontecimientos sucedidos el 11 de septiembre, ha decidido emplear las tecnologías necesarias para la prevención y, en su caso, represión de los delitos relacionados con organizaciones armadas con ese fin. Más allá de concederles a los gobiernos facultades para conservar los datos personales, se evita la inseguridad jurídica de los operadores encargados de tratar y almacenar aquéllos, estableciendo un catálogo de los datos que pueden ser objeto de retención.

---

(1) GÓMEZ NAVAJAS (2005): 33.
(2) STS de 3 de noviembre 1997, RA 8251, fundamento jurídico 10.º
(3) Por todos, TONIATTI (1996): 223, y PÉREZ LUÑO (1996): 567.
(4) MOLES PLAZA (2004): *in toto*.

La Directiva 2006/24 (5) tiene por objeto paliar de algún modo la inseguridad jurídica de los operadores, teniendo en cuenta la disparidad de legislaciones internas que tratan esta cuestión. La transferencia constante de datos de tráfico en el ámbito de la Unión, relativos a llamadas o a conexiones a Internet, exige que los operadores se sometan a una normativa homogénea en la materia y, como se examinará más adelante, se modulen de alguna manera el consentimiento informado del usuario y muchos de los principios relativos a la protección de datos, especialmente la calidad o la proporcionalidad, a efectos de alcanzar una mayor eficacia en la lucha contra la criminalidad en general y el terrorismo en particular. A tenor de la exposición de motivos de la Directiva, dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, «*es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo*».

A continuación se aborda el estudio de la protección de datos, tras la integración de las comunicaciones telefónicas, por Internet e inalámbricas o móviles en el mismo paquete regulador. Se analizarán, por tanto, los datos personales transmitidos a través de redes públicas de comunicaciones electrónicas. La Ley General de Telecomunicaciones las define como los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos, con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada (6). Posteriormente, se examinan las obligaciones que recaen sobre los operadores tras la entrada en vigor de la Directiva y, por último, el régimen de responsabilidades en caso de violación de las normas sobre protección de datos personales.

---

(5) Directiva 2006/24/CE, de 15 marzo, del Consejo, por la que se regula la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y modifica la Directiva 2002/58/CE, de 12 de julio de 2002, *DOL,* núm. 105, de 13 de abril de 2006, pág. 54.

(6) Anexo a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, *BOE,* núm. 264, de 4 de noviembre de 2003.

2. PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL: RASGOS GENERALES

El Tribunal Europeo de Derechos Humanos ha reiterado en diversas sentencias que la protección de los datos personales pertenece al ámbito de aplicación del derecho a la vida privada y familiar, reconocido por el Convenio Europeo de protección de los Derechos Humanos (7). Del mismo modo, la Carta de los Derechos Fundamentales de la Unión Europea recoge explícitamente esta circunstancia (8). En el ámbito interno, pese a que la Constitución omite toda referencia a la protección de datos, el Tribunal Constitucional la ha considerado un derecho fundamental autónomo respecto a la intimidad (9). De esta forma corrobora la ya plenamente asentada doctrina acerca de la autonomía del derecho a la protección de datos (10). El legislador, por su parte, ha contribuido a esclarecer, mediante una Ley Orgánica, los contornos y las garantías específicas inherentes a la protección de datos (11).

Los datos personales objeto de tutela son todos aquellos que identifican o permitan identificar a cualquier persona (12). Con arreglo a la jurisprudencia constitucional:

> «El objeto de protección del Derecho Fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual [...], sino los datos de carácter personal» (13).

Se trata de proteger, por lo tanto, «cualquier información», incluso aquella que en un inicio podría considerarse como irrelevante, pero que poniéndola en

---

(7) STEDH 28341/1995, de 4 de mayo de 2000, *Rotaru contra Rumania,* ap. 43.

(8) Artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000, *DOC,* núm. 364, de 18 de diciembre de 2000. Al respecto, véase LUCAS MURILLO DE LA CUEVA (2003): véase *www.madrid.org/comun/datos personales*.

(9) STC 292/2000, de 30 de noviembre, fundamento jurídico 6.º

(10) LUCAS MURILLO DE LA CUEVA (1990): 23, y PÉREZ LUÑO (1991): 37.

(11) LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *BOE,* núm. 298, de 14 de diciembre de 1999. A partir de ahora LOPD.

(12) STEDH 27798/1995, de 16 de febrero de 2000, *Amann contra Suiza* (ap. 65). STC 292/2000, de 30 de noviembre, fundamento jurídico 6.º Al respecto, véase también SAN de 24 de enero de 2003, Rec. 400/2001, fundamento jurídico 5.º, que se fundamenta en la sentencia constitucional aludida.

(13) STC 292/2000, de 30 de noviembre, fundamento jurídico 6.º

relación con otro tipo de datos puede dar un perfil completo de la persona (14). El derecho a la autodeterminación informativa, por tanto, se erige en la facultad de controlar todos los datos que se refieren a cada uno. Acoge tanto la potestad de imponer a terceros el deber de abstenerse de intromisión alguna en esta esfera, como la facultad positiva de controlar lo que ocurre con dichos datos, mediante el ejercicio del derecho de acceso, de rectificación, de cancelación, de información, de consentimiento y de oposición (15). En ese sentido, la información que se protege puede servir para confeccionar el perfil ideológico de la persona, racial, sexual, económico o de cualquier otra índole que, en determinadas circunstancias, puede constituir una amenaza para el individuo. La protección de los datos de carácter personal, como derecho autónomo, le permite a la persona controlar sus datos, para lo que se precisa su consentimiento para cualquier modificación o alteración de la finalidad para la que se emplean.

Esa amplia definición permite acoger todos los formatos en los que aparece la información y no es imprescindible que identifiquen clara e inequívocamente a su titular, sino que pueden ser datos que sirvan como medio para identificarlo. La identificabilidad aparece cuando de unos datos no se pueda deducir directamente la identidad de un sujeto, pero pueda resultar de una puesta en común o de la interrelación de dichos datos con otros. El criterio de la identificabilidad hay que entenderla como «razonablemente identificable», de tal manera que los supuestos en que la vinculación entre el titular de los datos y la información que se dispone para identificarlo requiera esfuerzos desproporcionados, no se podrá decir que se está ante datos personales estrictamente (16).

El afectado, como titular de los datos objeto de tratamiento (17), es la persona que se halla en condiciones de ceder los datos y acceder a la información acerca de su almacenamiento, tratamiento o transferencia (18). Todo ciudadano puede autorizar el tratamiento de sus datos personales mediante una manifestación de voluntad inequívoca, libre, específica e informada aquel de derecho (19). Ésta es la principal manifestación del principio de autodeterminación informativa o *habeas data* (20). Estas garantías incluyen el derecho a controlar su uso, aunque se inserten en un programa informático, o afecten a la salud de

(14) TÉLLEZ AGUILERA (2001): 64.

(15) STC 292/2000, de 30 de noviembre, fundamento jurídico 6.º

(16) Conclusiones y recomendaciones de la APD, en la inspección sectorial de oficio de «Concursos, juegos y sorteos de Televisión», *http://www.agpd.es/*.

(17) Artículo 3.*e)* LOPD.

(18) VIZCAÍNO CALDERÓN (2001): 72.

(19) Artículo 3 LOPD.

(20) MESSÍA DE LA CERDA BALLESTEROS (2003): 21.

los trabajadores (21). En cualquier caso, se exige que el ciudadano pueda conocer la existencia y los rasgos de esos ficheros y, sobre todo, el tratamiento que les dan las entidades públicas o privadas que los posean (22).

El derecho a la protección de los datos personales puede definirse como el poder de disposición sobre los mismos, y una de las facultades principales que compone dicho derecho, que consiste en conocer quién o quiénes los poseen, consiste en conocer cuál es la finalidad de su tratamiento y, en función de todo ello, la facultad de facilitarlos, modificarlos y eliminarlos (23). De aquí se desprende que, en un inicio, sólo mediante el consentimiento informado del ciudadano sus datos personales pueden ser tratados, conservados, modificados y eliminados. El Tribunal Europeo de Derechos Humanos ha exceptuado la necesidad de ese consentimiento en ciertos supuestos que han de preverse por Ley, siempre que esa medida sea estrictamente necesaria en una sociedad democrática. Además, el contenido de esa norma ha de ser previsible y fijar unas garantías adecuadas y suficientes contra los abusos (24). Así, como una de las excepciones, la Ley presupone que la firma de un contrato comporta la cesión, conservación y tratamiento de ciertos datos personales (25).

Una vez recabados los datos mediante cesión voluntaria u obligatoria, la entidad pública o privada que los posee (tenedor) ha de tratarlos conforme al principio de proporcionalidad. Eso significa que no pueden ser empleados para finalidades distintas de aquéllas para las que hubieran sido recogidos (26). Serán cancelados cuando los datos no sean necesarios para cumplir con la finalidad que motivó la recogida de los mismos. La vulneración de este principio conlleva la cancelación automática de los datos (27). Con carácter general, se prohíbe el tratamiento de los datos personales, cuando no exista una justificación que permita mantener los datos en el fichero, o cuando se están utilizando en contra del consentimiento manifestado por el afectado (28).

---

(21) STC 202/1999, de 8 de noviembre, fundamento jurídico 5.º Cítense, por todas, SSTC 30/1999, de 8 de marzo, fundamento jurídico único; 223/1998, de 24 de noviembre, fundamento jurídico único, y 198/1998, de 13 octubre, fundamento jurídico único.

(22) STC 254/1993, de 20 de julio, fundamento jurídico 7.º

(23) STEDH 23224/1994, de 25 de marzo de 1998, *Kopp contra Suiza,* ap. 53.

(24) STEDH 28341/1995, de 4 de mayo de 2000, *Rotaru contra Rumania,* ap. 59.

(25) Artículo 11 LOPD.

(26) Artículo 4.2 LOPD. Véanse SSTC 254/1993, de 20 de julio, fundamento jurídico 7.º, y 94/1998, de 4 de mayo, fundamento jurídico 4. º

(27) Artículo 4.5 LOPD.

(28) SAN (S. 3.ª) de 11 de mayo de 2001, Rec. 12/2000, y SAN de 6 de julio de 2001, Rec. 314/2000. Véase al respecto RUIZ CARRILLO (2001): 83.

La aplicación del principio de proporcionalidad implica siempre una ponderación de los bienes jurídicos en presencia. Por un lado, piénsese que la cesión o utilización de datos personales sin el consentimiento de su titular puede suponer un beneficio para facilitar, por ejemplo, la persecución de la criminalidad; por otro, ese sacrificio del derecho a la intimidad debería evitar un mal mayor que la violación del derecho del ciudadano a proteger sus datos personales (29). Este juicio valorativo resulta determinante para examinar si cualquier norma jurídica está privando de derechos a sus titulares más de lo estrictamente necesario para proteger intereses generales predominantes (30).

En el momento de resolver esos conflictos de bienes jurídicos, la Administración, el legislador o los jueces han de emplear numerosos criterios relacionados con las nuevas tecnologías, tal y como sucede cuando están involucradas la vida, la salud de las personas o los derechos de defensa en un procedimiento penal o sancionador (31). Dado el amplio margen de discrecionalidad para decidir caso por caso, ha de examinarse a fondo y de forma prudente el razonamiento lógico-jurídico que exponga la entidad responsable del tratamiento y conservación de los datos para permitir su tratamiento. Le corresponde a la Agencia de Protección de Datos inscribir en el Registro General el almacenamiento y archivo de datos, así como recibir las notificaciones relativas a las cesiones o su cambio de configuración (32).

3. PROTECCIÓN DE LOS DATOS PERSONALES EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS

3.1. *Servicios telefónicos*

Cada conexión a la línea telefónica y la correspondiente llamada es susceptible de registro en los nodos o conmutadores instalados por los operadores, a efectos de facturar los servicios a los usuarios o, en su caso, los servicios de interconexión ofrecidos y recibidos por otras compañías que explotan redes. Los números marcados, los destinatarios de las llamadas, la identificación del número al que llama así como la fecha y la hora de la comunicación son datos que se almacenan y retienen por los proveedores de redes y servicios para el

(29) STC 202/1999, de 8 de noviembre, fundamento jurídico 5.º Al respecto, MARROIG POL (2003): 542.

(30) ARZOZ SANTISTEBAN (2004): 267.

(31) ORTÍ VALLEJO (1994): 127.

(32) Artículo 26 LOPD.

pago de las contraprestaciones correspondientes, lo que incide en la protección de los datos y la intimidad de los clientes (33). Así se desprende de la jurisprudencia del Tribunal Europeo de Derechos Humanos, en virtud de la cual, cuando se empleen mecanismos técnicos que permitan registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato, sin que medie el consentimiento previo del titular de los mismos, puede violarse su derecho a la vida privada y familiar (34).

Tan sólo puede accederse a los datos referidos a una llamada telefónica en el supuesto en que una Ley así lo precise claramente y siempre que sea una medida estrictamente necesaria en una sociedad democrática. Este último requisito se cumple, a tenor del Tribunal Europeo de Derechos Humanos, siempre que «se rodee el sistema de vigilancia adoptado de garantías suficientes contra los abusos» (35). En los registros de las llamadas, efectuados con el objeto de facturar los servicios, se contienen informaciones —en especial, los números marcados— que son parte de las comunicaciones telefónicas. La obtención de todos esos datos puede encontrar su justificación en la persecución de presuntos criminales. Sin embargo, al tratarse de aspectos que afectan a la intimidad de las personas, debería solicitarse la preceptiva autorización judicial. La Corte Europea ya declaró que facilitar las informaciones acerca de los números llamados, sin el consentimiento del que realiza la llamada implica una violación de la vida privada y familiar, salvo que se rodee de las garantías suficientes (36), como la autorización judicial. El Tribunal Constitucional, de hecho, ha incluido en el ámbito del secreto de las comunicaciones «la identidad subjetiva de los interlocutores o corresponsales» (37).

Conforme al principio de proporcionalidad, el operador tan sólo podría ceder, modificar y, en general, emplear los datos relativos a las llamadas, únicamente con la finalidad de realizar gestiones propias del servicio, como la reclamación del pago, la emisión de las facturas o la reparación del mismo (38). Así se desprende de la normativa comunitaria (39), que exige informar a los

---

(33) STC 114/1984, de 29 de noviembre, fundamento jurídico 7.º Véanse sobre el particular R. MARTÍN MORALES (1995): 57, y RODRÍGUEZ RUIZ (1998): 68.

(34) STEDH de 2 de agosto de 1984, As. 8691/1979, *Malone contra Reino Unido,* ap. 81. Véase al respecto ARZOZ SANTISTEBAN (2004): 318.

(35) STEDH de 2 de agosto de 1984, As. 8691/1979, *Malone contra Reino Unido,* ap. 83.

(36) STEDH de 2 de agosto de 1984, As. 8691/1979, *Malone contra Reino Unido,* ap. 86.

(37) STC 114/1984, de 29 de noviembre, fundamento jurídico 7.º

(38) SAN de 18 de enero de 2002, Rec. 1096/2000, fundamento de derecho 2.º

(39) Directiva 2002/58, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas (Directiva sobre la Privacidad y las Comunicaciones Electrónicas), *DOL,* núm. 201/37, de 31 de julio de 2002.

afectados acerca de los datos de tráfico y la duración de su tratamiento (40). La Ley de Telecomunicaciones se remite, con carácter general, a la Ley Orgánica de Protección de Datos (41).

Con arreglo a lo declarado por la Agencia de Protección de Datos, la conservación de los datos referidos a las telecomunicaciones puede prolongarse hasta que no recaiga resolución definitiva en los litigios pendientes por impagos o, en su caso, hasta que no transcurran los tres meses que exige la legislación, como plazo para impugnar las facturas telefónicas por parte de los usuarios (42). Cuando se trate de datos de tráfico con fines de promoción comercial o para la prestación de servicios de valor añadido, los operadores podrán hacer uso de aquéllos durante el tiempo necesario para ello, siempre que medie el consentimiento informado por el usuario del servicio (43). El cliente dispone de un mes para prestar su consentimiento o negativa por vía postal o telefónica. Transcurrido ese plazo sin respuesta, se entiende que ha aceptado la utilización de sus datos para aquellos fines, siempre que la compañía le hubiera hecho constar este hecho.

El consentimiento tácito ha sido una figura muy controvertida, aunque parece que en última instancia ha tenido aceptación por la doctrina (44). Parece que la Ley Orgánica de Protección de Datos da también amparo a este tipo de consentimiento (45). Sin embargo, desde aquí no se entiende cómo se ha dado carta de naturaleza a una práctica que atenta contra el derecho a la protección de datos. Hay que tener en cuenta que el consentimiento tácito invierte la carga de actuación a la hora de requerir el consentimiento. Si bien la práctica obligatoria debería consistir en que el responsable del fichero tenga que actuar solicitando al titular de los datos su autorización, el consentimiento tácito hace que el que tenga que actuar para evitar que sus datos sean tratados sea el titular de los datos.

No es aceptable que el silencio juegue a favor del responsable del fichero. Si el derecho a la autodeterminación informativa supone el control del titular de los datos sobre los mismos, parece que el hecho de que el silencio juegue a favor

---

(40) Artículo 6 de la Directiva 2002/58.

(41) Artículo 34 de la Ley 32/2003.

(42) BRAVO-FERRER DELGADO (2000): 83, y DAVARA RODRÍGUEZ (2000): 29.

(43) Artículo 65.3 RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. *BOE,* núm. 102, de 29 de abril de 2005. A partir de ahora RCSU.

(44) DEL PESO NAVARRO (1998): *http://www.iee.es/*.

(45) El hecho de que en algunos artículos la LOPD exija el consentimiento expreso, artículo 7, hace pensar que en los demás casos cabe el consentimiento tácito.

del responsable del fichero puede suponer una minoración de las garantías que salvaguardan dicho derecho. La propia Audiencia Nacional ha entendido que el consentimiento tácito ha de ser interpretado con mucha cautela (46). Si se admite el consentimiento tácito, tendrá que ser con todas las garantías posibles para que el titular de los datos sepa cuáles son las consecuencias de su silencio. De acuerdo con la legislación de telecomunicaciones, los abonados deben disponer de un proceso sencillo y gratuito para retirar su consentimiento en cualquier momento (47).

Con la entrada de las nuevas tecnologías, los aparatos pueden disponer de mecanismos de identificación de llamada, es decir, pueden mostrar el número desde el que procede la llamada. En esos casos, se permitirá a los usuarios rechazar la identificación de las llamadas que se reciben o que se inician de forma temporal, y para cada conexión a la red o transmisión de una comunicación, mediante un procedimiento sencillo y gratuito (48). La normativa exige en todos esos casos a los proveedores de red que proporcionen la información necesaria a los abonados sobre la implantación de estos mecanismos de identificación, y que adviertan de la posibilidad de suprimir por el operador la identificación de llamada mediante procedimientos transparentes, cuando se trate de llamadas molestas o para atender situaciones de urgencia. Esta comunicación informativa se someterá a informe de la Agencia de Protección de Datos (49).

3.2. *Transmisión de datos: el problema de las conexiones a Internet*

La interdependencia entre servidores y redes pertenecientes a diferentes operadores y la posibilidad de que cualquier usuario se conecte con aquéllos comporta numerosos problemas de cara a una efectiva protección de los datos personales. El intercambio constante de flujos de información entre ordenadores puede suponer una cesión de los datos del usuario sin su constancia (50). En este punto cabe abordar el fenómeno de las *cookies*. Pueden definirse como archivos en los que figuran los datos del equipo que se conecta a la red. De este modo, al acceder a las páginas *web* o portales, cada ordenador transfiere a los servidores y a los sitios de almacenamiento (*hosting*) todos aquellos datos, con lo que los perfiles de la personalidad del usuario quedan perfectamente

(46) SAN de 21 de enero de 2004, fundamento jurídico 4.º
(47) Artículo 65.3 RCSU
(48) Artículos 8 de la Directiva 2002/58 y 70 RCSU.
(49) Artículos 10 de la Directiva 2002/58 y 71.2 RCSU.
(50) SÁNCHEZ BLANCO (2000): 36.

reflejados mediante los sucesivos recorridos que realiza a través de los sitios *web* (51).

Esta información resulta de enorme interés para las empresas, pues les permiten elaborar estudios de mercado o campañas de *marketing* (52). No obstante, todas esas informaciones se obtienen en franca vulneración de la Ley Orgánica de Protección de Datos, siempre que los usuarios no emitan un consentimiento informado. Tan sólo deberían utilizarse estos mecanismos con fines legítimos y con el conocimiento de los usuarios afectados (53). Los servidores introducen en los equipos aplicaciones específicas, preparadas para detectar los movimientos que realiza el usuario, ya que su dirección IP lo identifica automáticamente, quedando registrados los datos de cada visita a la página *web*. El archivo *cookie* puede contener la IP del usuario, que lo identificará inmediatamente, en caso de que haga uso de una IP fija. Estos registros de visitas son datos que se conservan por parte del que gestiona el sito *web*, sin que probablemente este último les haya notificado nada a los usuarios que han navegado a través de esas páginas. Si las direcciones IP permiten identificar a los usuarios, son datos personales que no pueden sustraerse a la Ley (54).

Las *cookies* dinámicas operan de forma diferente. Los archivos, transferidos a través de correos electrónicos o como consecuencia del acceso a páginas web o a portales, se instalan en el disco duro del ordenador del usuario, sin que medie el previo consentimiento de éste. De este modo, el archivo *cookie* almacena los sitios que ha visitado aquél (55). Algunos autores han calificado la información que circula por la red como «auténtica mercancía de datos», en su mayoría extraída sin el consentimiento de sus titulares. A las dificultades antedichas se añade el carácter global de Internet, lo que impide un control efectivo de las actividades de los servidores tanto por los usuarios como por la Administración encargada de la protección de los datos. La información no se almacena en ficheros localizados espacialmente, sino que se transfiere simultáneamente y en décimas de segundo a multitud de servidores y ordenadores, con lo que detectar el lugar y autores concretos que registran los datos constituye una misión muy complicada (56).

---

(51) ÁLVAREZ-CIENFUEGOS SUÁREZ (1999): 151.

(52) SÁNCHEZ BLANCO (2000): 36, y LANZOS SANZ (2003): *http://publicaciones.derecho.org/redi*.

(53) PRIETO ANDRÉS (2002): *www.laley.net/diario/diario_laley.html,* y RIBAS ALEJANDRO (2000): 165.

(54) OLIVER LALANA (2002): *www.laley.net/diario/diario_laley.html*.

(55) LLANEZA GONZÁLEZ (2000): 267.

(56) SÁNCHEZ BRAVO (2001): *www.laley.net/diario/diario_laley.html*.

Las violaciones de la legislación en materia de protección de datos pueden quedar impunes, ante la imposibilidad de localizar no ya la terminal, sino el servidor que almacena todas las informaciones. Esta circunstancia puede provocar que el usuario crea estar facilitando sus datos personales a una entidad cuando, en realidad, es otra, no identificada y radicada en otro territorio, la que está obteniendo aquéllos (57). Las compañías de *software* han introducido medios tecnológicos eficaces para contrarrestar los posibles defectos o agujeros que presenta la red. Sin embargo, no todos los usuarios que se conectan a Internet conocen la posibilidad de conseguir esos programas ni el modo de instalarlos. Al margen de ello, las aplicaciones informáticas evolucionan a marchas forzadas y la constante actualización de los programas antiespía también conlleva un considerable coste económico (58).

La problemática se agrava especialmente cuando los ataques a los ordenadores trascienden al mero espionaje y conllevan la comisión de delitos, como el acceso a la información estrictamente confidencial y el robo de números de tarjetas de crédito (59). El debate se sitúa en torno a la necesidad de que los usuarios dispongan de los medios tecnológicos más cualificados para preservar su intimidad, teniendo en cuenta que cualquier persona con conocimientos de usuario de Internet tiene a su alcance una legión de programas capaces de hacer estragos en equipos (60). Algunos virus pueden obtenerse en algunas páginas *web* (61). Una vez descargados, se manejan con la misma facilidad que cualquier otra aplicación (62).

En la actualidad la solución pasa por introducir mecanismos de autorregulación entre las empresas del sector y la firma de Acuerdos Internacionales, basados en el principio del puerto seguro (63). Las diferencias entre las legislaciones de los Estados, especialmente en el ámbito de la Unión Europea, contribuyen a demorar una regulación uniforme, sobre todo cuando los intereses empresariales transnacionales ejercen una notable influencia en las economías de Occidente. Aquéllas se benefician de estas transferencias ocultas acerca de los perfiles

---

(57) OLIVER LALANA (2002): *www.laley.net/diario/diario_laley.html*.

(58) SÁNCHEZ BRAVO (2001): *www.laley.net/diario/diario_laley.html*.

(59) *El País* de 6 de julio de 2005.

(60) MARTÍN-RETORTILLO BAQUER (2004): 553.

(61) Dictamen del Comité Económico y Social de 28 de junio de 2005: «Internet. Crea un programa comunitario plurianual para el fomento de un uso más seguro de Internet y las nuevas tecnologías en línea», *DOC,* núm. 157, de 28 de junio de 2005, pág. 136.

(62) ZAFRA (2004): *www.elpais.net*.

(63) MUÑOZ MACHADO (2000): 187, y ARRIBAS LUQUE (2002): *www.laley.net/diario/diario_laley.html*.

de cada usuario que accede a sus páginas web. La información puede resultar enormemente útil para sus estrategias empresariales (64).

3.3. *La Ley 25/2007* (65)*, relativa a la conservación de los datos personales en las comunicaciones electrónicas*

El texto legal tiene por objeto la transposición de la Directiva 2006/24 (66), que modifica el artículo 15 de la Directiva 2002/58, que contenía las garantías básicas en materia de protección de datos en el sector de las telecomunicaciones. Según el precepto mencionado, los Estados miembros pueden limitar el alcance de los derechos y obligaciones de los operadores de telecomunicaciones, que se basan en los principios de consentimiento informado y de proporcionalidad. Tales restricciones deben constituir medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas. Como ya se mencionó en la introducción, la existencia de un mercado único en el sector de las telecomunicaciones en el ámbito de la Unión requiere la aplicación de reglas uniformes por parte de las compañías para el almacenamiento de los datos personales de los usuarios (67).

Los Estados, no obstante, disponen de normativas muy diferentes, que permiten limitar el principio de consentimiento informado, en caso de preservar los fines de orden público antedichos. La Directiva 2006/24 tiene por objeto promover la seguridad jurídica entre los operadores, sin que éstos puedan verse sorprendidos por actuaciones sancionadoras de Estados en los que prestan sus servicios. Las previsiones comunitarias, en consecuencia, se destinan a fijar unas reglas precisas y uniformes en torno al tratamiento de los datos personales.

---

(64) PÉREZ LUÑO (1998): 729.

(65) Ley 25/2007, de 18 de octubre, de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, *BOE,* núm. 251, de 19 de octubre de 2007.

(66) Directiva 2006/24, de 15 de marzo, del Consejo, *DOL,* núm. 105, de 13 de abril de 2006, que regula la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y modifica la Directiva 2002/58/CE, de 12 de julio de 2002.

(67) HATZOPOULOS (1994): 85.

A) *Datos objeto de conservación*

A tenor de la Directiva, se incluyen en su ámbito de aplicación los datos relativos a las llamadas infructuosas, que se generan, tratan o conservan por operadores que estén bajo la jurisdicción de un Estado miembro (68). Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada (69). Los datos que han de ser conservados, tanto por operadores de redes como de servicios de comunicaciones electrónicas, se refieren al rastreo e identificación del origen de una comunicación tanto en redes fijas como móviles. En concreto, los números de teléfono y el nombre y dirección del abonado o usuario registrado. En el caso de que la señal proceda de Internet, los datos que resultan de obligada conservación son los siguientes, tanto para correos electrónicos como para llamadas telefónicas empleando el protocolo IP (70):

a) La identificación de usuario asignada.

b) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

c) El nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono.

En cuanto a la identificación del destino de la llamada, los operadores han de conservar los números y los nombres y direcciones referidos a las llamadas telefónicas. En el caso de que se establezca una comunicación por Internet o se realice una llamada telefónica a través de este medio, se conservarán la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet y los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación. También se registra la información relativa a la fecha y hora de la llamada o mensaje. En estos casos se obliga a retener los datos relativos a la fecha y hora del comienzo y fin de la comunicación.

Cuando se utilice el correo electrónico o la telefonía vocal por Internet: *a)* la fecha y hora de la conexión y desconexión del servicio de acceso a Internet,

(68) Artículo 3.2 de la Directiva 2006/24.
(69) Artículo 4.2 de la Ley 25/2007.
(70) Artículo 3 de la Ley 25/2007.

basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación y la identificación de usuario del abonado o del usuario registrado, y *b)* la fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario. En consecuencia, la Ley incluye en su ámbito de aplicación los datos necesarios para identificar el tipo de comunicación, que se refieren al servicio telefónico y al servicio de Internet utilizados.

Por otro lado, han de conservarse los datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1) Con respecto a la telefonía de red fija: los números de teléfono de origen y destino.

2) Con respecto a la telefonía móvil:

a) Los números de teléfono de origen y destino.

b) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

c) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

d) La IMSI de la parte que recibe la llamada.

e) La IMEI de la parte que recibe la llamada.

f) En el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3) Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

a) El número de teléfono de origen en caso de acceso mediante marcado de números.

b) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

A efectos de llevar a cabo una investigación criminal han de tenerse en cuenta los datos necesarios para identificar la localización del equipo de comunicación móvil:

1) La etiqueta de localización (identificador de celda) al comienzo de la comunicación.

2) Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

Se pretende distinguir entre los datos del tráfico (números, direcciones de correo electrónico, fechas, horas, etc.) y localización respecto al contenido de los mensajes, de modo que la Ley prohíbe la conservación de cualquier dato que revele el contenido de la comunicación (71). Asimismo, la conservación de todos ellos no puede resultar ilimitada en el tiempo, por lo que la Directiva fija un plazo mínimo de seis meses y uno máximo de dos años, contados a partir de la fecha de la comunicación (72). La decisión acerca del período preciso les corresponde a los Estados (73).

B) *Consecuencias de la nueva normativa*

Conforme a la Ley, la obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de los delitos (74). Ese plazo coincide con lo dispuesto en la Ley de Servicios de la Sociedad de la Información, que permite a los operadores retener hasta un máximo de doce meses los datos necesarios para la localización del terminal empleado por el usuario para transmitir cualquier comunicación por vía electrónica a título oneroso (75). En otras palabras, la utilización de Internet para transmitir mensajes de texto o de voz.

No obstante, aquella Ley ha de ser objeto de modificación, dado que la nueva Ley recoge con precisión todos los datos que han de conservarse por los operadores. No se limita a la localización del terminal, sino a su propietario, su número, la fecha y hora de la comunicación, etc., tal y como ya se ha aludido anteriormente. De hecho, la Ley, que transpone aquellos preceptos comunita-

---

(71) Artículo 3.2 de la Ley 25/2007.
(72) Artículo 6 de la Directiva 2006/24.
(73) DINIS NASCIMIENTO (2007): 73-90.
(74) Artículo 5.1 de la Ley 25/2007.
(75) Artículo 12 de la Ley 34/2002, de 11 de julio, *BOE,* núm. 166, de 12 de julio de 2002.

rios, contempla en su disposición derogatoria única la supresión del artículo 12 de la Ley de Servicios de la Sociedad de la Información, que versaba sobre la retención de datos.

Acerca de la conveniencia de la medida, se han escuchado voces contrarias a la conservación de los datos de tráfico por un plazo superior al estrictamente necesario para facturar las llamadas. Podría investigarse a personas que no hayan sido sospechosas previamente de ninguna actividad delictiva (76). Por otra parte, se ha afirmado que deberá tenerse en cuenta los enfoques menos invasores de la intimidad, por ejemplo, el procedimiento de *quick freeze* o congelación rápida (77). Mediante este mecanismo, ni los proveedores de comunicación ni los prestadores de servicios de Internet están obligados a almacenar datos relativos al tráfico. Por ejemplo, en casos justificados, las autoridades policiales consultan a las empresas y piden que se almacenen ciertos datos. Después de que éstos se hayan guardado, las autoridades tienen algunas semanas para recoger pruebas a fin de obtener una orden judicial. Posteriormente, con esta orden, pueden acceder a los datos.

Más allá del clásico debate que subyace en torno al dilema entre libertad y seguridad, la conservación de datos por los operadores durante un año puede entrañar un riesgo, no sólo para la intimidad de las millones de personas que se comunican por la red, sino también para la utilización de datos relativos a secretos comerciales u otro tipo de información confidencial (78). A fin de impedir que se cometan abusos en la conservación de los datos, se ha propugnado establecer unas garantías específicas. Entre ellas cabe citar la aplicación del principio de proporcionalidad, es decir, que la conservación de los datos se destine exclusivamente a la persecución de la delincuencia organizada y los delitos de terrorismo (79). Eso excluye que el tratamiento y la extracción de toda la información contenida en ellos se refiera a personas que se hallan al margen de cualquier sospecha sobre la participación en esos actos. De lo contrario podría

---

(76) Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM (2005) 438 final], *DOC,* núm. 298/1, de 29 de noviembre de 2005, pág. 4.

(77) Dictamen 4/2005, de 21 de octubre de 2005, sobre la propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM (2005) 438 final, de 21 de septiembre de 2005].

(78) Dictamen 4/2005, pág. 6.

(79) Dictamen 4/2005, pág. 9.

atentarse contra su intimidad (80). Por otro lado, los datos conservados sólo podrán ser cedidos previa autorización judicial (81).

Sin embargo, ¿cómo pueden las autoridades policiales o de investigación distinguir entre las diferentes llamadas, si precisamente una investigación consiste en plantear todas las hipótesis? La nueva Directiva puede desembocar en una peligrosa espiral. Si se admite que cualquier pista en una investigación puede resultar necesaria para la persecución de un tipo determinado de delincuencia, entonces inevitablemente la conservación puede salpicar a personas que simplemente han mantenido un contacto, aunque sea casual o inesperado, con miembros o presuntos integrantes de bandas armadas o terroristas. Al margen de que ello puede entorpecer la investigación, se podrían causar daños y perjuicios a la imagen y reputación de personas que simplemente aparecen en un listado de llamadas o en un directorio de correo electrónico.

Las facultades de conservación otorgadas a los operadores de comunicaciones electrónicas conllevan la aplicación de la Ley de Protección de Datos y, en concreto, los principios de consentimiento informado y proporcionalidad. En cuanto al primero, los operadores deberían señalar en las cláusulas contractuales que todos los datos mencionados serán objeto de conservación durante el plazo establecido por la Ley, a los efectos que en ella se contemplan, es decir, la persecución de la criminalidad. Asimismo, han de notificar fehacientemente a todos sus clientes actuales el período de tiempo del almacenamiento de esos datos, a efectos de que puedan ejercer un control sobre los mismos.

En cuanto al segundo, la compañía de servicios de comunicaciones electrónicas de que se trate no puede cederlos o utilizarlos para fines distintos a la persecución de aquellos delitos, lo que plantea el nada desdeñable debate acerca de la definición de criminalidad organizada o bandas terroristas. Esta cuestión queda fuera del alcance del ciudadano medio, puesto que los parámetros para precisar la existencia de aquel tipo de delincuencia se encuentran a disposición de los cuerpos especializados en investigación policial. Además, la cesión ha de ser requerida por las autoridades públicas previstas en la Ley. En concreto, podrán solicitar esa información, con arreglo a la Ley, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado cuando desempeñen funciones de policía judicial, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera en el desarrollo de sus competencias como policía judicial y el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre

(80) PÉREZ LUÑO (2005): 22.
(81) Artículo 6.1 de la Ley 25/2007.

personas o entidades, siempre que dispongan de la preceptiva autorización judicial (82).

En otro orden de consideraciones, la Ley incluye en su ámbito de aplicación a los operadores de redes (83). Ello se debe a que éstos también registran todos los datos relativos a los números marcados, las direcciones, la fecha de las llamadas, su localización y duración, a fin de facturar los servicios de interconexión que puedan prestar a otros operadores. El problema se presenta en el momento en que el usuario desconoce que el recorrido de su mensaje puede atravesar redes explotadas por operadores a los que no se halla vinculado por ninguna relación contractual. Eso significa que también ignora que existen datos almacenados por diferentes compañías, con lo que se quiebra de alguna forma el principio de autodeterminación informativa.

Así, el usuario no podrá disponer y vigilar el uso de sus datos, lo que puede provocar que los proveedores de redes y servicios cedan o utilicen aquéllos sin conceder al ciudadano la posibilidad de conocer que los datos, referidos a las comunicaciones que realizan, pueden ser almacenados por operadores de red diferentes al que le presta el servicio telefónico. Tampoco dispondrán de la capacidad para identificar el responsable de la correspondiente infracción administrativa. Idéntica problemática se suscitaría en las comunicaciones por Internet o correo electrónico, cuyos datos de identificación del remitente y del receptor del mensaje son conservados en diferentes servidores. La única solución consiste en que los abonados sean informados acerca de todas estas cuestiones, ya sea mediante la inclusión de alguna cláusula contractual, ya sea mediante la notificación personal a los que ya han suscrito el contrato.

4. CONCLUSIONES

El constante flujo de datos en las comunicaciones electrónicas encierra controversias no poco relevantes en la aplicación de la legislación sobre protección de datos. Al encaminar la señal o facilitar la conexión a los usuarios, los operadores registran toda la información esencial a efectos de facturar las tarifas del servicio a los usuarios o los precios de interconexión al resto de operadores. Por ejemplo, la identidad del que origina la llamada, el destinatario, la localización, etc. Por si pudieran suscitarse dudas en torno a la tutela de todos estos datos al abrigo del derecho a la vida privada y familiar, el Tribunal Europeo de

(82) Artículo 6 de la Ley 25/2007.
(83) Artículo 2 de la Ley 25/2007.

Derechos Humanos ya se ha pronunciado en el sentido de que una cesión de todos ellos sin el consentimiento de sus titulares o afectados puede suponer la violación del derecho humano mencionado. Postura ésta que ha acogido el Tribunal Constitucional, en relación con el derecho fundamental a la intimidad.

La limitación de estos derechos tan sólo puede emanar de una Ley lo suficientemente precisa como para establecer garantías que eviten su utilización abusiva. La legislación de telecomunicaciones debe complementarse con la Ley Orgánica de Protección de Datos, de modo que cada uno de los operadores debe confeccionar un fichero y registrar los datos correspondientes a cada uno de los abonados, además de poner en marcha un registro de las llamadas efectuadas por los usuarios, a efectos de facturar los pagos referidos a la prestación de servicios y a la interconexión. Los operadores pueden almacenar y tratar toda esa información en la medida necesaria para exigir las prestaciones derivadas del servicio. Los usuarios, por su parte, han de conocer la existencia de esos ficheros, que almacenan tanto sus datos personales como los relativos a las llamadas efectuadas. De este modo, podrían hacerse efectivos los principios de proporcionalidad y de consentimiento informado.

La Ley 25/2007 ha exceptuado la aplicación de estas normas propias de la protección de datos en los supuestos en que éstos sirvan para la persecución de delitos graves, de la criminalidad organizada o de grupos terroristas. Además, los operadores de redes y de servicios se ven obligados a conservar los datos que circulan por la red, relativos a los números o direcciones electrónicas, la duración de las comunicaciones, identidad de los que inician la comunicación y los destinatarios e, incluso, datos referentes a la localización de los mismos. El período durante el que han de almacenarse oscila, en función de la legislación interna de cada Estado, entre seis meses y dos años. Eso significa que los operadores deben advertir a los usuarios que toda esa información será almacenada durante ese período de tiempo, a fin de que aquéllos puedan comprobar que no se utilizan para fines distintos a la investigación criminal del corte ya aludido. La principal problemática en este punto se halla en que la extracción o transferencia de datos puede salpicar a personas que han mantenido contactos esporádicos y sin ninguna relación con el delito que se pretende perseguir.

Al interconectarse redes explotadas por distintos operadores, las llamadas pueden discurrir por diferentes redes, con lo que aquéllos son los encargados del registro y el tratamiento de los datos mencionados. Esta cuestión ha de advertirse a los abonados, a efectos de que puedan ejercer sus derechos de cancelación, rectificación, consulta y control de aquéllos. Del mismo modo, podrían comprobar que todos los operadores de red han adoptado las medidas necesarias para el cumplimiento de la Ley. El incumplimiento del deber de advertir a los usuarios la posibilidad de que aquellos datos pueden ser almacenados por operadores a los que no ha

otorgado expresamente el consentimiento constituye una infracción de las normas sobre protección de datos. Por tanto, sería conveniente incluir esta información en las cláusulas contractuales de las pólizas, a efectos del cumplimiento de la Ley.

BIBLIOGRAFÍA

ÁLVAREZ-CIENFUEGOS SUÁREZ, José María (1999): *La Defensa de la Intimidad de los Ciudadanos y la Tecnología Informática*, Pamplona, Aranzadi.

ARRIBAS LUQUE, José María (2002): «Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los Estados Unidos: el sistema de principio de puerto seguro», *La Ley,* núm. 5497.

ARZOZ SANTISTEBAN, Xavier (2004): «Art. 8. Respeto a la vida privada y familiar», en LASAGABASTER, Iñaki (dir.): *Convenio Europeo de Derechos Humanos. Comentario Sistemático*, Madrid, Civitas, págs. 267 y sigs.

BRAVO-FERRER DELGADO, Miguel (2000): «Protección de los datos personales en el sector de las telecomunicaciones», *Gaceta Jurídica de la Competencia y de la Unión Europea,* núm. 208, págs. 83 y sigs.

DAVARA RODRÍGUEZ, Miguel Ángel (2000): *La Protección de los Datos Personales en el Sector de las Telecomunicaciones*, Madrid, Universidad Pontificia de Comillas, pág. 29.

DEL PESO NAVARRO, Emilio (1998): «¿De quién son nuestros datos?», *En Línea,* núm. 19, en *http://www.iee.es/*.

DINIS NASCIMIENTO, Rui (2007): «La Directiva sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones: ¿gran hermano o seguridad colectiva?», *REDETI,* núm. 28, págs. 73-90.

GÓMEZ NAVAJAS, Justa (2005): *La Protección de los Datos Personales*, Cizur Menor, Thomson-Civitas y APDCM, pág. 33.

HATZOPOULOS, Vassilis (1994): «L'open Network Provision (ONP): moyen de la déregulation», *Revue Trimestrelle de Droit Communautaire,* núm. 30, págs. 85 y 86.

LANZOS SANZ, Antonio (2003): «La protección jurídica de los datos personales en el sector de las telecomunicaciones», *REDI,* núm. 117. Véase en *http://publicaciones.derecho.org/redi*.

LLANEZA GONZÁLEZ, Paloma (2000): *Internet y Comunicaciones Digitales*, Barcelona, Bosch, pág. 267.

LUCAS MURILLO DE LA CUEVA, Pablo (1990): *El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales Frente al Uso de la Informática,* Madrid, Tecnos.

— (2003): «La primera jurisprudencia sobre el derecho a la autodeterminación informativa», *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid,* núm. 1. Véase *www.madrid.org/comun/datos personales*.

MARROIG POL, Lorenzo (2003): «La seguridad nacional y el acceso a los datos de tráfico de las comunicaciones electrónicas», *La Ley,* núm. 5579, de 10 de junio de 2003.

MARTÍN-RETORTILLO BAQUER, Lorenzo (2004): «Consideraciones comunes a los artículos 33, 34 y 35», en GARCÍA DE ENTERRÍA, Eduardo, y DE LA QUADRA-SALCEDO, Tomás (coords.): *Comentarios a la Ley General de Telecomunicaciones (Ley 32/2003),* Madrid, Civitas, pág. 553.

MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto (2003): *La Cesión o Comunicación de Datos de Carácter Personal*, Madrid, Thomson-Civitas y APDCM, pág. 21.

MOLES PLAZA, Ramón Jordi (2004): *Derecho y Control en Internet. La Regulabilidad de Internet,* Barcelona, Ariel.

MUÑOZ MACHADO, Santiago (2000): *La Regulación de la Red. Poder y Derecho en Internet*, Madrid, Taurus, pág. 187.

OLIVER LALANA, Ángel Daniel (2002): «El derecho fundamental virtual a la protección de datos. Tecnología transparente y normas privadas», *La Ley,* año XXIII, núm. 5592.

ORTÍ VALLEJO, Antonio (1994): *Derecho a la intimidad e informática (tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada),* Granada, Comares, pág. 127.

PÉREZ LUÑO, Antonio Enrique (1991): *Derechos Humanos, Estado de Derecho y Constitución,* 4.ª ed., Madrid, Tecnos.

— (1996): *Manual de Informática y Derecho*, Barcelona, Ariel.

— (1997): «Internet y el Derecho», *Informática y Derecho, Revista Iberoamericana de Derecho Informático,* núm. 19-22, pág. 728.

— (1998): «Internet y Derecho», *Revista Iberoamericana de Derecho Informático,* núm.19-22, pág. 729.

— (2005): «Internet y la garantía de los derechos fundamentales», VVAA, *Estudios Jurídicos sobre la Sociedad de la Información y Nuevas Tecnologías*, Universidad de Burgos, pág. 22.

PRIETO ANDRÉS, Antonio (2002): «La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones», *La Ley,* año XXIII, núm. 5620.

RIBAS ALEJANDRO, Javier (2000): «Riesgos legales en Internet. Especial referencia a la protección de datos personales», *REDETI,* núm. 3, pág. 165.

RODRÍGUEZ RUIZ, B. (1998): *El secreto de las Comunicaciones: Tecnología e Intimidad*, Madrid, McGraw-Hill, pág. 68.

RUIZ CARRILLO, Antonio (2001): *La Protección de los Datos Personales,* Barcelona, Bosch, pág. 83.

SÁNCHEZ BLANCO, Ángel (2000): *Internet. Sociedad, Empresa y Poderes Públicos*, Granada, Comares, pág. 36.

SÁNCHEZ BRAVO, Álvaro (2001): «Una política comunitaria de seguridad en Internet», *La Ley,* núm. 5414.

TÉLLEZ AGUILERA, Alberto (2001): *Nuevas Tecnologías, Intimidad y Protección de Datos. Estudio Sistemático de la Ley Orgánica 15/1999*, Madrid, Edisofer, pág.64.

TONIATTI, Roberto (1991): «Libertad Informática y Derecho a la Protección de Datos Personales: Principios de Legislación Comparada», *RVAP,* núm. 29, págs. 34-56.
VIZCAÍNO CALDERÓN, Miguel (2001): *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas.
ZAFRA, Ignacio (2004): «Troyanos al alcance de cualquiera», *El País*.

RESUMEN

Este trabajo tiene por objeto profundizar en las consecuencias jurídicas que producen las nuevas tecnologías en la protección de datos personales en el ámbito de la Unión Europea. Por un lado, diversos operadores de telefonía pueden conservar los datos de los usuarios, relativos al sujeto que realiza la llamada, al destinatario, la localización, la fecha y la hora de la misma. Esto se debe a que toda esta información se almacena por las compañías, a efectos de exigir los pagos por interconexión entre sus redes. Los usuarios deberían conocer qué operadores poseen todos aquellos datos, cuáles son y para qué los emplea. De lo contrario, se estaría infringiendo la legislación de protección de datos. Por otro lado, los mecanismos tecnológicos que permiten almacenar una enorme cantidad de información se han convertido en medios para burlar la legislación sobre protección de datos. Por ejemplo, las *cookies* son archivos que se introducen en los ordenadores de los usuarios, sin su consentimiento, a fin de controlar los hábitos de navegación. Todo ello con efectos comerciales, como la preparación de estrategias de *marketing*.

PALABRAS CLAVE: nuevas tecnologías, Internet, protección de datos, llamadas telefónicas, correo electrónico, consentimiento de los usuarios, conservación de los datos.

ABSTRACT

This article has the purpose of studying the impact of new technologies in data protection in the European Union. On one hand, many operators can use data which refer to the people who call by phone, that's to say, who receives those calls and when are made. Taking account these operators manage a net that is interconnected with others, users should know different companies must retain data during a period of time. On the other hand, Internet and new technologies, that allow hosting much information, are ways to breach the legislation on data protection. For example, cookies are files that are introduced in computers to control and view the web pages visited by the users. In this way, companies and operators can manage personal data without affected citizens' consent. User can't exercise the right to change and remove their data. Data protection legislation states that holders of particulars have the right to supervise the objective for using data.

KEY WORDS: new technologies, Internet, data protection, telephone calls, electronic mail, users' consent, retain data.