Revista de Estudios Económicos y Empresariales
Núm. 25, 2013, pp. 205-244 - ISSN: 0212-7237

COMERCIO ELECTRÓNICO Y PROTECCIÓN DE DATOS

VIRGINIA VEGA CLEMENTE
Doctora en Derecho. Abogada

ÍNDICE: 1. **RESUMEN-SUMMARY. 1. COMERCIO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN.- 2. LA PROTECCIÓN DE DATOS EN LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE.- 3. ÁMBITO DE APLICACIÓN DE LA LEY ESPAÑOLA.- 4. PRINCIPIOS IMPERANTES EN MATERIA DE PROTECCIÓN DE DATOS. 4.1. Principio de calidad de datos. 4.2. El deber de información. 4.3. El requisito del consentimiento. 4.4. Deber de seguridad de datos. 4.5. Deber de secreto. 4.6. Derecho a impugnar valoraciones. 4.7 Derecho de indemnización.- 5. INFRACCIONES Y SANCIONES.- 6. CONSIDERACIONES GENERALES SOBRE TRATAMIENTOS DE DATOS EFECTUADOS A TRAVÉS DE INTERNET. 6.1. Consideraciones generales. 6.2. La protección de datos de carácter personal y el uso de *cookies.***

RESUMEN

Las nuevas tecnologías han revolucionado el mundo de la información y las comunicaciones y han propiciado la existencia de un mercado abierto y global. La contratación electrónica permite realizar contratos relativos a la prestación de bienes y servicios con ventajas evidentes: mayor competitividad, reducción de costes y mayor celeridad en las relaciones comerciales. Junto a estas ventajas, hemos de señalar que el nuevo sistema contractual plantea problemas que afectan a la protección de los derechos de los consumidores. Por eso es necesario definir los límites de acceso a la intimidad y el respeto a los derechos de la persona humana, entre los que se encuentran en nuestro ordenamiento jurídico la Ley Orgánica 15/1999, de 13 de diciembre, sobre protección de datos de carácter personal, y la normativa que la desarrolla.

Palabras claves: Sociedad de la información, Comercio electrónico, Derechos de la personalidad, Derecho a la intimidad, Derecho Mercantil.

Clasificación JEL: K29

SUMMARY

The new technologies have revolutionized the world of information and communication so they have led to the existence of an open and global market. E-procurement allows contracts for the provision of goods and services with clear advantages: increased competitiveness, cost reduction and faster trade relationships, . Along with these advantages, we note that the new system raises contractual issues affecting the protection of consumer rights. Therefore it is necessary to define the limits of access to privacy and respect for the rights of the human person, including those found in our legal Organic Law 15/1999, of December 13, about the protection of personal data and implementing regulations.

Keywords: Information Society, Electronic commerce, Civil Laws, Privacy, Commercial Law.

JEL classification: K29

1. COMERCIO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN

El desarrollo de las nuevas tecnologías genera una clara amenaza para la privacidad de los ciudadanos en general, y de los consumidores y usuarios en particular. Las telecomunicaciones permiten a los proveedores recoger, analizar, almacenar y usar la información con gran facilidad y eficiencia[1]. Su uso meramente comercial puede propiciar la utilización en otros ámbitos sociales y con otras finalidades, por lo que se pone de relieve el nacimiento de un nuevo problema en el tratamiento y respeto de datos personales: la necesidad del establecimiento de mecanismos para protección en sus diferentes etapas[2]. Esto es, desde la recogida, pasando por el tratamiento y almacenamiento, hasta su posible cesión a terceros; y todo ello con independencia del soporte en que se encuentren[3].

Tanto el comercio tradicional como el comercio electrónico exigen la identificación de todas las personas que participan en el mismo. Esta aparente similitud oculta, no obstante, cuestiones a considerar que representan un serio peligro para salvaguardar la intimidad del consumidor en el tráfico jurídico económico moderno. Así, la necesidad de que los datos circulen por la red[4], la imposibilidad de conocer el uso que el receptor de datos va a hacer de los mismos o la consideración de que una acumulación de datos va a permitir, mediante el estudio sociológico o de otra índole, trazar el perfil de una persona,

[1] MUNAR BERNAT, P. A., "Protección de datos en el comercio electrónico", en *Comercio Electrónico y Protección de los consumidores* (Coord. G. A. Botana), Ed. La Ley, Madrid, 2001, pág. 275. V. también DRUMMOND, V., *Internet, Privacidad y Datos personales,* (Traducción de I. Espín Alba), Ed. Reus, Madrid, 2004, págs. 40 y ss.

[2] La necesidad de la protección del derecho a la intimidad y la problemática planteada en las distintas etapas que facilita la circulación por la Red, a pesar de una protección más adaptada y poco eficaz, es puesta de relieve por FRAYSSINET, J., "La protection des donés personnelles est-elle assurée sur l´internet?, en *Le droit international de l´internet* (Dirc. G. Chantillon), Ed. Bruylant, Bruxelles, 2002, págs. 435 y ss.

[3] ROSSELLÓ MORENO, R., *El comercio electrónico y la protección de los consumidores,* Ed. Cedecs Derecho, Barcelona, 2001, pág. 130.

[4] "La prassi del commercio elettronico è, senza dubbio, caratterizzata da numerose occasioni di racolta dei dati personali del navigatore –consumatore `virtuale´, ora paleti –mediante la richiesta di compilazione di generici formulari elettronici o di veri e propri ordini di beni o servizi –ora oculte- sin pensi al caso emblemático del `Data Log´ e dei `cookie´ (TOSI, E., "La tutela dei data personali", en *I problemi giuidici di Internet,* 3ª ed., cit., pág. 314.

nos indican que, al final, podrán ser utilizados con fines espurios[5]. Las técnicas informáticas con su capacidad de proceso pueden ejercer, por tanto, un control social e interferir en la vida de las personas sin que éstas lleguen a percibirlo[6]. Este necesario intercambio de datos en el proceso de construcción de la sociedad de la información hace posible que las nuevas tecnologías sean un factor que facilite la violación de derechos fundamentales de los individuos, lo que motiva que los Estados tengan que tomar conciencia de la necesidad de tutelar estos derechos y proteger la intimidad de las personas[7].

Frente a esta práctica han reaccionado las legislaciones estatales a fin de garantizar el derecho fundamental de la protección de los datos, que tiene como finalidad específica proporcionar a la persona un poder de control sobre cualquier tipo de dato personal, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho afectado[8]. A tales fines nos encontramos con dos sistemas jurídicos contrapuestos. De un lado, el seguido en los Estados Unidos de Norteamérica que ha implantado un sistema poco intervencionista, inspirado en presupuestos liberales[9]. Y de otro, la Unión Europea[10], que ha impulsado otro de corte más social, y que pone de relieve una

[5] MUNAR BERNAT, P., *op. cit.,* pp. 276-277; DRUMMOND, V., *op. cit.,* págs. 54 y ss.

[6] Cfr. VEGA VEGA, J. A., *Contratación electrónica y protección de los consumidores,* Ed. Reus, Madrid, 2005, págs. 357-358.

[7] G. GORASANITI trata el problema de la epistemología jurídica de la seguridad jurídica afirmando que el reconocimiento de la vulnerabilidad es un factor de seguridad. *Videri Esperienza giuridica e sicurezza informatica,* Giuffrè editore, Milano, 2003, págs. 28 y ss. y 73 y ss.

[8] BARRIUSCO RUIZ, C., *La contratación electrónica,* 2ª ed., cit., pág. 425. DAVARA RODRÍGUEZ, M. A., *Manual de Derecho Informático,* Ed. Aranzadi, Pamplona, 2002, pág. 47, define como protección de datos "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".

[9] Un estudio práctico sobre los problemas planteados por la vulneración del derecho a la intimidad en Estados Unidos, puede verse en BABIRAK/ALBERT/VANGELLOW/SHAHEEN, "Electronic Commerce in USA", en *E-Commerce in the World. Aspects of Comparative Law,* págs. 317 y ss.

[10] Sobre la protección de datos personales en la Unión Europea existe una vasta literatura jurídico-comunitaria: HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esto datos,* Aranzadi, Pamplona, 1997; ESTADELLA YUSTE, O., "The Draft Directive of the European Community Regarding the Protection of Personal Data",

especial sensibilidad por la protección de la intimidad[11] y los datos personales de sus ciudadanos. Entre nosotros, la Constitución, en su artículo 18.1, establece como garantía fundamental la protección al honor, la intimidad personal y familiar y a la propia imagen, subrayando en el ordinal 4º del precepto que la "ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Debido a que nos movemos en una economía globalizada, también en el ámbito internacional[12] se suscitó pronto la urgencia de regular el régimen de tutela de los datos de carácter personal[13]. La propia Organización de Naciones

Internacional and Comparative Law Quarterly, vol. 41, enero 1992, págs. 170-179; HEREDERO HIGUERAS, M., "El mercado único europeo y la protección de datos personales informatizados. Observaciones sobre el borrador de Directiva marco de protección de datos (SYN 287)", *Computerworld,* 1991; ALONSO BLAS, D., *La aplicación de la directiva europea de protección de datos en España: reformas necesarias en la L.O.R.T.A.D.,* Encuentro sobre Informática y Derecho, Aranzadi, Madrid, 1996; MARTÍN-CASALLO, J. J., "La Directiva 95/46/CE y su incidencia en el ordenamiento jurídico español", *Jornadas sobre el Derecho Español de la protección de datos personales,* Agencia de Protección de Datos, Madrid, 1996; HOLMES, B. P., "US criticizes EC Data Directive´s Potencial Burdens and Barriers", *Transnational Data and Communications Report,* vol. XIV, núm. 6, 1991, págs. 8-9; BLUME, P., *Comments on the atended proposal for a Council Directive on protection of personal data,* Universidad de Copenhague, Instituto de Ciencia Jurídica, B, núm. 48; DAVARA RODRÍGUEZ, M. A., *Guía práctica de la protección de datos,* Ed. Asnef Equifax, Madrid, 1999; IDEM, *La protección de datos en Europa: principios, derechos y procedimiento,* Ed. Asnef Equifax, Madrid, 1998; FERNÁNDEZ SAMANIEGO, J., "La Nueva Ley de Protección de Datos de Carácter Personal Española (Ley Orgánica 15/1999, de 13 de diciembre)", en *REDI,* Núm. 24, julio 2000; PÉREZ DE VELASCO, J. R., "Protección de Datos de Carácter Personal", en REDI, núm. 27, octubre 2000; PRIETO ANDRÉS, A., "La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones", *Diario La Ley,* año XXIII, núm. 5260, 26 de septiembre de 2002, págs. 1 y ss.; SÁNCHEZ ALMEIDA, C./MAESTRE RODRÍGUEZ, J. A., *La Ley de Internet. Régimen jurídico de los Servicios de la Sociedad de la información y Comercio Electrónico.* Ed. Servi DOC, Barcelona, 2002, pág. 151; SÁNCHEZ CARAZO, C/SÁNCHEZ CARAZO, J. M., *Protección de datos de carácter personal relativos a la salud,* Ed. Agencia de Protección de Datos, Madrid, 1999; VAT CUTSEN/WITTAMER/MARNET et alt., *E-Commerce in the World,* Ed. Bruylanbt, Bruxelles, 2003, págs. 20-28.

[11] Tal como pone de relieve con un recorrido normativo e histórico WALDEN, I., "Data protection", en *Computer Law* (editada por C. Reed y J. Angel), 5ª ed, Oxford University Press, 2003, págs. 419-421.

[12] WALDEN, I., "Data protection", en *Computer Law* (editada por C. Reed y J. Angel), 5ed, cit., págs. 421 y ss.

[13] Cfr. GOURION, P.A./RUANO-PHILIPPEAU, M., *Le droit de l´Internet dans l´entreprise,* Ed. L.G.D.J., París, 2003, pág. 49.

Unidas recogió ciertos principios rectores que, andando el tiempo, fueron la base de la legislación actual. A escala internacional destaca el Convenio número 108, de 28 de enero de 1981, del Consejo de Europa[14].

La Unión Europea -y, por ende, todos los Estados miembros- se ha preocupado de establecer una normativa que, a la par de potenciar el comercio electrónico y mejorar el intercambio de información en nuestra sociedad, sirva para tutelar el respeto a datos íntimos y personales con el designio de proteger la privacidad[15].

Así, tenemos en primer lugar la Directiva 95/46/CE del Parlamento 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[16], que instaba a los Estados miembros a garantizar los derechos y

[14] Nos referimos al Convenio 108, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, celebrado en Estrasburgo el 28 de enero de 1981, ratificado por España en el año 1985 y publicado en el BOE núm. 274, de 15 de noviembre de 1985, cuyo fin se establece en el artículo 1 del mismo, como "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencial, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona." Hasta la promulgación de la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, (L. O. R. T. A. D.), nuestro país ha venido incumpliendo algunas de las obligaciones jurídico-internacionales establecidas en su texto normativo, referidas precisamente a la elaboración y aprobación de la mencionada legislación interna y explicitadas en el artículo 4 del Convenio. El Convenio trata de armonizar "los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos" sobre la base de una serie de principios como la recogida lícita de datos, la calidad y confidencialidad de los datos sensibles, la información de la persona implicada y los derechos de acceso y de rectificación, ahora bien, siempre desde el convencimiento de que se trata de un Convenio de mínimos. Es por ello que el Convenio pretende compatibilizar en todo momento la protección del derecho a la intimidad personal con la liberalización de los flujos de datos entre Estados partes, siendo así que la libre circulación de los datos de carácter personal entre los Estados signatarios sólo decaerá en dos supuestos: 1) Cuando la protección de los datos de carácter personal no sea equivalente en la otra parte y 2) Cuando la transmisión de los mismos se realice a un tercer Estado que no sea parte en el Convenio.

[15] Sobre el papel de las telecomunicaciones y la sociedad de la información en el ámbito europeo, puede verse: ORTIZ BRU, C., "La política Europea en materia de telecomunicaciones. Hacia la sociedad de información", en *Contratación y Comercio Electrónico,* (Dir.: F.J. Orduña), Tirant lo Blanch, Valencia, 2002, págs. 771 y ss.

[16] Sobre la importancia y repercusiones de esta Directiva a nivel europeo y especialmente en Italia, puede verse TOSI, E., "La tutela dei data personali", en *I problemi giuidici di Internet,* 3ª ed., Giuffrè Editore, Milano, 2003, págs. 334 y ss.

libertades de las personas físicas en lo que respecta al tratamiento de los datos personales y en especial su derecho a la intimidad, de forma que los datos puedan circular libremente en la Unión. Esta normativa originó en nuestro país la publicación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que nació con el propósito de aplicarse al régimen de los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de los mismos por los sectores públicos y privados.

La Ley española no es un dechado de virtudes, y se han impuesto todo tipo de críticas, sin que debamos omitir que muchas también son positivas[17]. Así, entre las que miran su aspecto más positivo destaca el esfuerzo que supone introducir en nuestra cultura jurídica actual nuevos valores sobre la defensa de la intimidad de los ciudadanos y consumidores, principales roles impuestos por el mercado y los poderes públicos. En el lado contrario hemos de subrayar que la Ley cae con demasiada frecuencia en la ambigüedad y en la falta de precisión de muchos términos y situaciones que regula[18]. Así como que de un análisis conjunto de sus preceptos se colige una estructura bastante asistemática, con la dispersión en distintos preceptos de principios e instituciones que regula[19].

La tutela inspirada por la Unión Europea se amplió al sector de las telecomunicaciones con 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. Esta Directiva tenía como finalidad proteger, como complemento de la Directiva 95/46/CE, los derechos fundamentales de las personas físicas y, en particular, el derecho a la intimidad, así como los intereses legítimos de las personas jurídicas. Pero la evolución tecnológica, las nuevas tecnologías digitales avanzadas y, sobretodo, la creciente utilización de Internet como infraestructura mundial

[17] Es sabido, aunque no por ello debe obviarse, que el proceso de confección de la LOPD vino acompañada de circunstancias que incidieron en su confección y que dieron como resultado el empleo de una técnica legislativa poco rigurosa. Véase MARTÍNEZ MARTÍNEZ, R. Y CHAVELI DONET, E., "A propósito del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Comentarios a un seminario de la UIMP", Agencia de Protección de Datos de la Comunidad de Madrid, 2005, núm. 16.

[18] SÁNCHEZ ALMEIDA, C. /MAESTRE RODRÍGUEZ, J.A., *La Ley de Internet. Régimen jurídico de los Servicios de la Sociedad de la Información y Comercio Electrónico,* Ed. Servidoc, Barcelona, 2002, pág. 151.

[19] VEGA VEGA, J. A., *Contratación electrónica y protección de los consumidores,* cit., pág. 361.

para la prestación de una gama de servicios de comunicaciones electrónicas incrementaron los riesgos para los datos personales y la intimidad de los consumidores. De donde se impuso la necesidad de garantizar una mayor protección, pero también que ésta se realizara de una forma armónica, con el fin de impedir que surgieran de las diversas legislaciones obstáculos al desarrollo y a la prestación de nuevos servicios en el mercado interior.

Con estas premisas se publica la Directiva 2002/58/CE del Parlamento y del Consejo, de 12 de julio de 2002[20], sobre la privacidad y las comunicaciones electrónicas, que deroga la Directiva 97/66/CE y complementa la 95/46/CE. La transposición al derecho interno del nuevo régimen de esta Directiva ha tenido lugar mediante la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones[21].

La actual Ley Orgánica 15/1999, a fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos[22], 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los

[20] La Directiva 2002/58/CE se fundamenta en el hecho de que la precedente Directiva 97/66/CE debía ser adaptada al desarrollo de los mercados y de las tecnologías para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de las comunicaciones electrónicas disponibles al público fuera el mismo, con independencia de las tecnologías utilizadas, de ahí la necesidad de derogarla y sustituirla. Y en este afán, la Directiva 2002/58/CE pretende armonizar las disposiciones de los Estados miembros necesarios para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales y del sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Unión Europea. Esta Directiva se aplica a los servicios de comunicaciones electrónicas públicos, por cuanto los no públicos quedarán cubiertos por la Directiva 95/46/CE.

[21] Cfr. VEGA VEGA, J. A., "Comunicaciones comerciales por vía electrónica", en *Revista General de Legislación y Jurisprudencia,* núm. 4, octubre-diciembre 2003, págs. 627 y ss.

[22] La Agencia es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas. Su regulación se contiene en los artículos 35 y ss. de la LOPD y en el Real Decreto 428/1993 de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. BOE 106 de 4.5.1993.

datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario, con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

En este contexto nace el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado mediante el Real Decreto 1720/2007. Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo. Se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema[23].

De todo lo dicho llegamos a la conclusión de que, para que el desarrollo de las nuevas tecnologías sea positivo, es necesario ofrecer a los usuarios una protección adecuada de su intimidad[24]. En efecto, para que el comercio electrónico

[23] El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

se desarrolle, tanto los consumidores como los empresarios deben tener confianza en que sus transacciones no serán interceptadas ni modificadas y crear este clima de confianza es una condición previa para que se acuda a esta modalidad de transacción. Sin embargo, está muy extendida la inquietud respecto a la protección de la intimidad y los datos personales, que se agudiza cuando la transacción se hace a través de fronteras[25]. La protección de la intimidad y de los derechos a ella ligados plantea retos cada vez más novedosos, en la medida en que las nuevas tecnologías de la información permiten no sólo nuevas formas de comunicación, sino también, paralelamente, más modos de interceptar las comunicaciones.

Es evidente que la utilización de las nuevas tecnologías que están en la base del comercio electrónico supone un menoscabo del ámbito de la privacidad, ya que permiten que los datos puedan ser obtenidos, compilados y almacenados sin dificultad y configurar un perfil del usuario de estos medios, accediendo al conocimiento de actitudes, gustos o hábitos, que deberían permanecer, salvo que uno dispusiera lo contrario, en la esfera de la privacidad. La legislación más estricta pierde valor en la medida en que es posible eludirla mediante el uso de nuevas tecnologías.[26] Los prestadores de servicios de la sociedad de la información al usar los datos recabados del destinatario de su servicio deben sujetarse a una serie de limitaciones y deberes.

Para fijar estas limitaciones y deberes, siempre que se trate de los servicios de acceso a Internet[27], será de ayuda la Ley General de Telecomunicaciones[28],

[24] Aunque caben muchas interpretaciones, siguiendo a GALLO RUIZ, G. y otros, en *Protección de Datos Personales: Soluciones en Entornos Microsoft,* Microsoft Ibérica S. R. L., Madrid, 2003, pág. 17, podemos definir el derecho a la intimidad "como el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, de sus sentimientos, de sus emociones, de sus datos biográficos y personales de su imagen […] abarca muchas circunstancias de la vida personal".

[25] *La Firma y el Comercio Electrónico. Aspectos jurídicos de los servicios de la sociedad de la información.* Asociación de Internautas (España). Documentos sobre Comercio Electrónico. <http//:www.internautas.org/documentos/mj_firmacomer.htm.>

[26] En este sentido, ANN CAVOUKIAN, PH. D., que en la ponencia presentada en la XX Conferencia Internacional de Autoridades de Protección de datos, celebrada en 1998 mantiene que la normativa por sí misma no es suficiente para proteger el derecho a la intimidad en el próximo siglo y será necesario completar la legislación, en particular con herramientas de carácter tecnológico (herramientas de protección de la intimidad, PET), que en algunos casos constituirán el medio esencial de protección disponible, en todos los sentidos, verdaderamente significativo.

[27] Cfr. artículo 1.2, párrafo 2, de la Ley General de Telecomunicaciones.

que es de aplicación a los servicios de comunicaciones electrónicas (art. 1,1 de la Ley General de Telecomunicaciones)[29].

Entrando en un análisis normativo, diremos que el marco habilitante del desarrollo de la normativa sobre protección de datos de carácter personal nos lo proporciona nuestra propia Constitución que, en su artículo 18.4, establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". En concomitancia con lo anterior, la legislación general sobre la protección de datos será de total aplicación a los servicios de la Sociedad de la Información.[30] De esta manera será también de aplicación el Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000[31], sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y los Organismos de la Comunidad y sobre la libre circulación de esos datos. El Reglamento se ocupa del tratamiento de datos personales por parte de Instituciones y Organismos Comunitarios. Las instituciones y los organismos creados por los Tratados constitutivos de las Comunidades Europeas o en virtud de dichos Tratados[32] garantizarán, de conformidad con el Reglamento, la protección de los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, y no limitarán ni prohibirán la libre circulación de datos personales entre ellos o entre ellos y destinatarios sujetos al Derecho nacional de los Estados miembros adoptado en aplicación de la Directiva 95/46/CE. La autoridad de control independiente establecida por el

[28] Cfr. art. 34,1º LGT. En la Exposición de Motivos de la Ley General de Telecomunicaciones se dice que esta norma incorpora, entre otras, la Directiva 2002/58/CE, 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).

[29] Véase el artículo 1.1 de la Ley General de Telecomunicaciones.

[30] Considerando 14 de la 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, DOL 178 de 17 de julio de 2000.

[31] Confróntese el Considerando (5) del Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

[32] En lo sucesivo denominados «instituciones y organismos comunitarios».

Reglamento, en lo sucesivo denominada «Supervisor Europeo de Protección de Datos», supervisará la aplicación de las disposiciones del presente Reglamento a todas las operaciones de tratamiento realizadas por las instituciones y organismos comunitarios.

Como hemos adelantado anteriormente, una de las normas que se revelan de gran importancia para el comercio electrónico es la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas)[33], que viene a derogar a la Directiva 1997/66/CE[34], ya que se necesita un marco jurídico neutro y flexible que no se vea obsoleto por el desarrollo tecnológico, como ha sido el caso; y por ello lo primero que se hace es cambiar el término de telecomunicaciones por el de comunicaciones electrónicas, concepto mucho más amplio, neutro y flexible.

Esta Directiva, que se aplica a los servicios de comunicaciones electrónicas públicos –los no públicos quedarán cubiertos por la Directiva 95/46/CE-, tiene por objeto reducir al mínimo necesario el tratamiento de datos personales y que la información sea tratada de forma anónima mediante pseudónimos cuando sea posible. Uno de los objetivos principales es crear normas que sean neutras con respecto a la tecnología, es decir, que no impongan la utilización de un tipo concreto de tecnología ni discriminen en su favor, sino que garanticen que un

[33] Es la última directiva aprobada del denominado paquete Telecom que impulsó el Consejo Europeo de Lisboa de marzo de 2000 (Bol. 3-2000 punto 1.6). Las restantes son: Directiva 2002/19/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados y a su interconexión (directiva acceso), Directiva 2002/20/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (directiva autorización), Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (directiva marco), y Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (directiva servicio universal). Todas ellas publicadas en DOL 108 de 24 de abril de 2002. Posteriormente la Comisión ha dictado la Directiva 2002/77/CE de la Comisión de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas DOL 249 de 17.09.2002, para adaptarse al nuevo marco regulador creado por las Directivas anteriormente mencionadas.

[34] 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.

mismo servicio quede regulado de forma equivalente con independencia del medio a través del que se preste. Esto significa que los consumidores y usuarios deben gozar del mismo nivel de protección con independencia de la tecnología a través de la cual se proporciona el servicio.

2. LA PROTECCIÓN DE DATOS EN LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE

En lo tocante a ámbito de tutela, señala el artículo 2.1 que se aplica a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. De ello se deduce que se exige como mínimo la intervención de dos sujetos: uno, el que trata los datos (el responsable del tratamiento o del fichero[35]); otro, cuyos datos son objeto de tratamiento (el afectado o interesado[36]). Es decir, la LOPD se aplica cuando una persona trata datos que hacen referencia a otra distinta. La misma considera "dato de carácter personal" a cualquier información concerniente a personas físicas identificadas o identificables, y protege estos datos en orden a su "tratamiento", que no es otra cosa que las operaciones y procedimientos técnicos de carácter automatizado, o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

[35] Los términos *responsable del tratamiento y responsable del fichero* son sinónimos. Podemos definirlos como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. En un principio hubo cierta confusión al emplear el legislador en unos casos responsable del fichero y en otros del responsable del tratamiento, pero se trata del mismo sujeto al que el legislador se le había ocurrido nombrar de dos formas diferentes. Se trata de la posibilidad de que los datos personales puedan ser tratados por personas distintas de los usuarios de la propia organización del responsable del fichero, por encargo de éste. Esta tercera persona se convierte en este caso en *responsable del tratamiento y responsable del fichero,* y presta servicios al responsable del fichero, siempre que dichos servicios tengan como objeto una finalidad lícita y legítima. En estos casos, la Ley Orgánica 15/1999 regula la relación entre el responsable del fichero y el encargado del tratamiento, estableciendo una serie de obligaciones encaminadas a garantizar la seguridad del tratamiento de los datos personales.

[36] Los términos *afectado e interesado* son sinónimos y se refieren a cualquier persona física cuyos datos son tratados. Se define en el artículo 3 como la "persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo."

Los antecedentes a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), los encontramos en la Ley Orgánica 5/1992, de 29 de octubre, Reguladora del Tratamiento Automatizado de Datos (LORTAD)[37]. Posteriormente, la Ley fue derogada con la entrada en vigor de la LOPD, ya que la LORTAD es anterior a la Directiva 1995/46/CE. Por esta razón se hizo necesario o bien adecuar la norma a lo dispuesto en la Directiva, o bien, como al final fue el caso, aprobar una nueva disposición.

En el artículo 1º de la ley se establece que el fin pretendido por la misma es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Esta manifestación se ha visto reforzada por la Sentencia del Tribunal Constitucional –STC 292/2000 de 30 de noviembre- la cual establece que el derecho a la protección de datos es un derecho, que sin estar recogido expresamente en la Constitución, goza del rango de derecho fundamental autónomo, que tiene su justificación en la llamada libertad informática y el derecho a impedir o restringir el uso de datos personales para un uso diferente al que justificó su obtención; es decir, atribuye a la persona un derecho de uso y destino sobre sus datos[38].

[37] La LORTAD fue publicada como consecuencia de la ratificación por el Reino de España del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, firmado en Estrasburgo por el Plenipotenciario de España el 28 de enero de 1982, el cual dispone que los estados signatarios quedan obligados a desarrollar una ley que proteja los datos de carácter personal. No ha sido éste el único acto del Consejo de Europa, puesto que ha elaborado una larga serie de Recomendaciones y Resoluciones en la materia. Éstas pueden ser consultadas en: DAVARA RODRÍGUEZ, M. A., *Manual de Derecho Informático,* Aranzadi 2002, págs. 56 y ss.

[38] "Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18,1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico. Ahora bien, con la inclusión del vigente art. 18,4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad funda-

Como bien señala algún sector de la Doctrina, lo que se establece es un derecho de autodeterminación de la persona, que reconoce a su titular, la facultad de decidir cuándo y cómo está dispuesta a permitir que sea difundida su información personal o a difundirla ella misma, esto es, la facultad de la persona de controlar y conocer los datos que sobre ella se encuentran en soportes físicos[39].

Como consecuencia de estas afirmaciones, llegamos a la conclusión de que no debemos entender el derecho a la protección de datos, como así continua rezando la sentencia del Constitucional, como una vertiente del derecho a la intimidad, sino que esa protección se extiende a cualquier tipo de dato personal, íntimo o no, público o privado, ya que, por el hecho de que un dato personal sea público, no escapa del poder de disposición de su titular. Es más, ese derecho se amplía a todos los datos que identifiquen o permitan identificar a una persona, pudiendo servir para la confección del perfil ideológico, racial, sexual, económico o de cualquier índole.

Continuando con el planteamiento de la situación, hemos observado que el artículo 2.1 establece que la ley será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Para entender esta disposición, se impone ya la necesidad de definir "dato de carácter personal", y "tratamiento". Por *dato de carácter personal* entendemos, según el artículo 3.a), cualquier información concerniente a personas físicas identificadas o identificables[40]. Por *tratamiento* entendemos, según el artículo 3.c): las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como, las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Prácticamente nada escapa al control de esta Ley, ya que entran dentro del ámbito de aplicación legal los tratamientos de datos no automatizados (por

mental" (STC 254/1993, de 20 de julio, FJ 6). Véase también SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2).

[39] DAVARA RODRÍGUEZ, M. Á., Aranzadi, Pamplona, 2008, pág. 58.

[40] Se plantearon dudas sobre sí la dirección de correo electrónico o e-mail constituye un dato de carácter personal. En este sentido se pronuncia la Agencia de Protección de Datos (APD) en su Memoria de 2000, página 338 indicando que, si la información está constituida por un conjunto de signos que permiten la vinculación directa o indirecta con una persona física, debe entenderse que constituye un dato de carácter personal.

ejemplo en soporte papel, aunque hasta el 24 de octubre de 2007 estaban exentos de cumplir ciertas obligaciones de la ley, según reza la disposición adicional primera) y la ley se aplica tanto a los tratamientos de titularidad pública como privada (en este concepto deben agruparse las empresas y profesionales liberales).

Es más, aunque la LOPD extiende su ámbito de protección a las personas físicas, se planteó la duda de sí un empresario o profesional liberal que no revistiera su actividad bajo la forma de empresa, estaba o no protegido por la LOPD. Tras una serie de vaivenes iniciales, la APD ha entendido a raíz de la Resolución que dictó el 27 de septiembre de 2001, que habrá que analizar cada caso concreto, viendo si cabe diferenciar entre la actividad empresarial o profesional, y la propiamente privada de ese individuo en cuestión; es decir, ver si los datos personales han sido tratados sólo por su consideración de empresario o profesional liberal[41]. En esta misma línea se encuentra la Sentencia de la Audiencia Nacional de 11 de octubre de 2002, que obliga a diferenciar si el dato se refiere a la persona-empresa o a la persona, estando protegidos si es imposible diferenciar su actividad mercantil de su propia esfera de actividad.

3. ÁMBITO DE APLICACIÓN DE LA LEY ESPAÑOLA

En este epígrafe abordaremos las reglas que otorgan competencia a la LOPD. Esto es, cuándo se entiende que es de aplicación la legislación española. No olvidemos que, en un mundo internacionalizado, los datos de las personas fluyen por todo el globo terráqueo (pensemos en una transferencia de fondos de un banco a otro, sólo por poner un ejemplo).

Estas reglas son las siguientes: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento[42]. b) Cuando al responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española en aplicación de normas de derecho internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en el territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

[41] Para más información, véase Memoria de la APD de 2001 y APARICIO SALOM, J., *Estudio sobre la Ley de Protección de Datos de Carácter Personal,* Aranzadi, 2ª Edición, 2002, págs. 41 y ss.

[42] Véase el art. 3 d) de la LOPD.

Por su parte, se establecen una serie de excepciones a la aplicación de la LOPD, unas de exención y otras de remisión a la normativa específica. Empezando por las primeras, no se aplicará la LOPD a: a) A los ficheros[43] mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domesticas. b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de la delincuencia organizada. No obstante, en esos supuestos, el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos (APD).

Se regirán por su normativa específica y por lo especialmente previsto, en su caso, por esta Ley, los siguientes tratamientos de datos personales: a) Los ficheros regulados por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del Régimen del personal de las Fuerzas Armadas. d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes. e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

4. PRINCIPIOS IMPERANTES EN MATERIA DE PROTECCIÓN DE DATOS

La LOPD establece en su Título II, bajo la expresión "**Principios de la protección de datos**" una serie de criterios o reglas que deben regir toda actividad de tratamiento de datos de carácter personal.

[43] Atendiendo al artículo 3 b), entendemos por este: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización o acceso. El concepto que utiliza la APD de fichero implica que debe estar organizado de modo que permita su acceso y consulta conforme a un criterio lógico y determinado (numérico, alfabético...) Memoria de la APD del 2000, página 54.

4.1. PRINCIPIO DE CALIDAD DE DATOS

El primero es el principio de calidad de los datos. En virtud de esta disposición, los datos de carácter personal sólo se podrán recoger y someter a tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. De la misma manera, una vez obtenidos, no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido obtenidos. La única excepción es su mantenimiento posterior por fines históricos, estadísticos o científicos. A la vista de esta disposición, se puede plantear el lector la tremenda ambigüedad de ésta, ya que habrá que delimitar caso por caso y sector por sector, qué datos son pertinentes, adecuados y no excesivos. Pero en aras de intentar clarificar esta norma, indicaremos que en la práctica se ha demostrado que puede salvarse.

La LOPD establece que los datos deben ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado[44]. En el caso de resultar inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correctos.

Los datos deberán ser cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la que hubieran sido requeridos o recogidos. Asimismo, los datos deberán ser almacenados de manera que permitan el ejercicio del derecho de acceso, salvo que legalmente sean cancelados.

La LOPD, en aras a preservar adecuadamente la finalidad de almacenamiento de datos, prohíbe expresamente que se recojan datos por medios fraudulentos, desleales o ilícitos.

4.2. EL DEBER DE INFORMACIÓN

Otro de los deberes que impone la LOPD es el deber de información en la recogida de datos[45]. En virtud del mismo, los interesados deberán ser previa-

[44] Según el artículo 3 e), afectado o interesado es: la persona física titular de los datos que sean objeto del tratamiento al que se refiere el apartado c) del presente artículo.

[45] Para tratar datos de un tercero es preciso, en primer lugar, recopilarlos. Pues bien, cuando el responsable de un tratamiento pretende recopilar datos de un tercero o los recopila tiene la obligación de informar de ciertos detalles del tratamiento al afectado. Este deber no es exclusivo del responsable del tratamiento, ya que el prestador de servicios de la sociedad de la

mente informados a la recogida de sus datos personales, de modo expreso, preciso e inequívoco en los siguientes aspectos: de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información[46], del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas[47], de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante[48].

Solamente deberán constar las advertencias primera y última si el resto de advertencias se deducen claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Se establece, igualmente, que esta información deberá constar de manera claramente legible si para la recogida de datos se utilizan cuestionarios u otros impresos.

Eso sí, si los datos no se han obtenido directamente del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del fichero o por su representante[49], dentro de los tres meses siguientes al

información por el hecho de ser prestador también debe informar al destinatario del servicio de algunos aspectos relacionados con el prestador y con el servicio que éste presta.

[46] Artículo 5.1.a LOPD. El conocimiento de la finalidad del tratamiento resulta esencial para poder ejercitar el derecho a la protección de datos personales, ya que los principios de la LOPD se articulan en torno a la finalidad del tratamiento.

[47] Esta información sólo procede cuando se obtienen los datos directamente del afectado.

[48] Artículo 5,1, e LOPD. Esta obligación adquiere gran relevancia si nos encontramos en el sector del comercio electrónico. Como ha tenido ocasión de manifestar la APD en "Recomendaciones de la APD al sector del Comercio Electrónico, para la adecuación de su funcionamiento a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal", es necesario informar en todo momento de la identidad del responsable del tratamiento, sobre todo si se ha llegado a esa página a través de un hiperenlace. Por ello es necesario informar al usuario de modo inequívoco que el control va a transferirse a otra Web. La LSSICE también exige expresamente que el destinatario del servicio pueda acceder fácilmente al nombre y denominación social del prestador de servicios, su residencia y domicilio, o en su defecto, la dirección de uno de sus establecimientos permanentes en España. La identidad (y dirección) del responsable y de su posible representante resultan importantes porque conocer al responsable del tratamiento podría resultar decisivo a los efectos de que el afectado preste su consentimiento o no, y porque el afectado tiene que conocer ante quién ejercitar sus derechos.

[49] Para garantizar el correcto cumplimiento del deber de informar al afectado, la LOPD establece que cuando el responsable de tratamiento no esté establecido en territorio de la UE, y utilice en el tratamiento de datos medios situados en territorio español, deberá designar a un representante en España, salvo que tales medios se utilicen con fines de tránsito.

registro de los datos, salvo que ya hubiera sido informado con anterioridad en los términos analizados anteriormente. De esto se deduce que, si por ejemplo, un familiar facilitó los datos de carácter personal y estos fueron recogidos en un cuestionario que informaba en los términos establecidos legalmente, y se entregó una copia del mismo al familiar, el interesado ya habrá sido informado previamente[50].

Lo anteriormente dispuesto no será de aplicación cuando así lo disponga una ley, el tratamiento tenga una finalidad histórica, estadística o científica o cuando la obligación de información resulte imposible o exija esfuerzos desproporcionados en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, eso sí, la interpretación de esta disposición queda al criterio de la APD u organismo autonómico equivalente. Si los datos proceden de fuentes accesibles al público y se destinan a la actividad de publicidad o prospección comercial, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

Esta obligación de información, tiene su origen en la intención de evitar vicios del consentimiento, y más en concreto un vicio en la prestación del consentimiento[51], ya que el consentimiento es otro de los derechos que asisten a los afectados, y está íntimamente ligado al derecho de información.

4.3. EL REQUISITO DEL CONSENTIMIENTO

Como acabamos de manifestar, otro derecho íntimamente ligado al de información, es el del consentimiento[52]. A tenor del artículo 6, se establece que el tratamiento de datos requerirá el consentimiento[53] inequívoco del afectado,

[50] En cambio, en la LSSICE, el deber de informar se cumple con permitir el acceso de forma permanente, fácil, directa, gratuita a la información (artículo 10.2).

[51] Véase APARICIO SALOM, *Estudio sobre la Ley de Protección de Datos de Carácter Personal,* Aranzadi, 2ª Edición, 2002, páginas 94 y ss.

[52] Uno de los grandes principios por los que se rigen los tratamientos de datos personales de terceros es el principio de autodeterminación, por el cual el responsable del fichero debe obtener el consentimiento del afectado para poder tratar sus datos.

[53] El consentimiento, como regla general, también se exige cuando el responsable del tratamiento pretende comunicar los datos a un tercero (artículo 11,1 de la LOPD). El artículo 3,1 de la LOPD define cesión o comunicación de datos como "[…] toda revelación de datos realizada a una persona distinta del interesado". La LOPD regula los movimientos de carácter

salvo que la ley disponga otra cosa. Por consentimiento, a efectos de la LOPD entendemos: toda manifestación de voluntad, libre inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le concierna. Atendiendo a esta definición, se ha planteado la duda de cual es la forma en la que debe manifestarse ese consentimiento, si de forma expresa o si cabe también la presunta. La APD ha otorgado validez a estas formas de prestar el consentimiento, apoyándose en el artículo 7 que exige el consentimiento expreso para cierto tipo de datos, que serán analizados en breve. En suma la Agencia de Protección de Datos entiende que si para cierto tipo de datos, que gozan de la condición de especialmente protegidos, se requiere por la LOPD el consentimiento expreso, para el resto de datos valdrá cualquier forma de manifestación de la voluntad admisible en derecho[54].

Las excepciones[55] a este derecho vienen recogidas en el apartado siguiente del artículo 6, y son las siguientes:

1ª. Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Como bien señala APARICIO SALOM[56], la LOPD permite una serie de tratamientos no consentidos, como el que puede establecerse ante la AEAT, ya que prevalece el deber público sobre la propia privacidad.

2ª. 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. Se entiende para estos casos que el consentimiento se encuentra subsumido en el otorgado para la obligación principal.

3ª. Cuando el tratamiento de los datos tenga la finalidad de proteger un interés vital del interesado, en los términos del artículo 7, apartado 6 de la pre-

---

internacional de datos a países que *no proporcionen un nivel de protección equiparable al que presta la LOPD.* El art. 33 de la LOPD prevé, entre otros requisitos, una autorización previa de la Agencia de Protección de datos. El régimen jurídico previsto en el artículo 33 de la LOPD no será aplicable "cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista" (artículo 34,2,e de la LOPD).

[54] Para más información, véase APARICIO SALOM, ob. ult. cit., páginas 70 y ss.

[55] Para estos casos, y siempre que una ley no disponga lo contrario, el afectado podrá oponerse al tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero viene obligado a excluir del tratamiento los datos relativos al afectado.

[56] Ob. ult. cit., páginas 32 y ss.

sente ley (prevención y diagnostico medico, asistencia sanitaria...). En este caso prevalecen los derechos a la vida y a la salud sobre el de la privacidad.

4ª Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Con carácter general, indicaremos que el consentimiento podrá ser revocado cuando exista causa justificada para ello, no pudiendo atribuírsele efectos retroactivos.

4.4. DEBER DE SEGURIDAD DE DATOS

Especial mención merece el deber de seguridad de los datos. En virtud del artículo 9 se establece que el responsable del fichero, y en su caso el encargado de tratamiento (figura que analizaremos con detalle más adelante), deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico natural. En consecuencia, no se pueden registrar datos de carácter personal en ficheros que no reúnan las condiciones determinadas por vía reglamentaria con respecto a su integridad y a su seguridad y a la de los centros de tratamiento, locales, equipos y programas.

Para dar cumplimiento a esta disposición, y aprovechando la habilitación fijada en la ley, para que por reglamento se regulen estos requisitos de seguridad, ha podido mantenerse el Real Decreto 994/1999 de 14 de junio, de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (RMS). Este reglamento fue dictado en amparo de la LORTAD, pero a escasos meses de la aprobación de la LOPD, opción que no resulta muy lógica si tenemos en cuenta que la LORTAD sólo regulaba los tratamientos automatizados y, por el contrario la LOPD se ocupa de cualquier fichero recogido en soporte físico (por lo que cabe incluir también aquellos ficheros tratados en soporte papel, que como consecuencia de ello se encuentran excluidos del ámbito de aplicación del RMS).

4.5. DEBER DE SECRETO

Una vez sentados los principios anteriores, pasamos a mencionar otro de los deberes que establece la LOPD, deber que no es otro que el de **secreto**. En virtud de éste, el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal (entre los que podemos incluir al encargado de tratamiento, figura que se analizará a continuación), están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Estas obligaciones subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. De lo anteriormente dicho se deducen dos cosas, la primera es que a tenor de esta disposición el personal que trabaje para el responsable del fichero está sujeto a las obligaciones mencionadas, y segundo, que esa obligación persiste inclusive finalizada la relación laboral o mercantil que los unía.

Según establece la LOPD la comunicación de datos es toda revelación de datos realizada a persona distinta del interesado, mencionaremos que para que esta comunicación de datos a un tercero sea válida, debe realizarse para cumplir los fines directamente relacionados con las funciones legítimas del cedente y cesionario, previo consentimiento del cedente. No obstante, este consentimiento no será necesario si la cesión está autorizada por una ley, si los datos están recogidos de fuentes accesibles al público y cuando el tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. Para que sea válida en este caso, la cesión ha de limitarse a la finalidad que se justifique. Tampoco será necesario prestar consentimiento cuando la comunicación deba efectuarse al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen encomendadas. Tampoco será necesario cuando la comunicación se dirija a instituciones autonómicas análogas al Defensor del Pueblo y Tribunal de Cuentas. Estarán exentas igualmente las comunicaciones entre Administraciones Públicas que tengan por objeto el tratamiento posterior con fines históricos, estadísticos o científicos, ni cuando los datos sean relativos a la salud, y esa cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

El consentimiento será nulo cuando la información facilitada al interesado

no le permita conocer la finalidad a la que se destinan sus datos, o el tipo de actividad de aquel a quién se pretenden comunicar. Para la APD[57], para que sea válido se debe informar claramente al interesado sobre el destino de sus datos, siendo nulas las fórmulas genéricas (entre las cuales cabe incluir las de cesión de datos al grupo de empresas, para los cuales, se entiende que, aunque integrados en un grupo, cada empresa goza de personalidad jurídica propia). Este consentimiento tiene, como no podía ser de otra manera, carácter revocable. No obstante, todo lo dicho no será aplicable si previamente a la comunicación de datos, se lleva a la práctica un procedimiento de disociación de datos. Este procedimiento, según queda definido por la ley, consiste en todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. Para dar cuerpo a esta previsión, la APD[58] manifestó que si los datos personales van unidos a un Código, y ese Código puede a posteriori ser asociado a una persona identificada o identificable, no estamos ante datos disociados. De esto se deduce que si queremos disociar los datos, el procedimiento ha de ser tal que no puedan volver a asociarse.

Para los ficheros de titularidad privada, se plantea una especialidad, ya que según dispone la LOPD, el responsable del fichero deberá informar a los afectados en cuanto se produzca la primera cesión de datos. Este deber de información abarcará la finalidad del fichero, la naturaleza de los datos que han sido cedidos y la dirección del cesionario. El responsable del tratamiento no vendrá obligado a cumplir esta disposición cuando la cesión venga impuesta por una ley, cuando los datos hayan sido previamente disociados, y cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En ese caso la cesión será legítima, si se limita a la finalidad que la justifica. También estará el responsable de tratamiento exento si la comunicación tiene por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas u organismos autonómicos equivalentes, en el ejercicio de sus funciones. La última excepción es la que se fundamenta en una cesión de datos entre Administraciones Públicas con el objeto del tratamiento posterior de datos con fines históricos, estadísticos o científicos.

Existe una categoría especial de datos que se denominan datos especial-

[57] Véanse Memorias de la APD de 2000 y 2001.

[58] Memoria 2000, pág. 100.

mente protegidos. Esta diferenciación se apoya en el artículo 16.2 de la Constitución española, según el cual nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. De esta forma sólo podrán tratarse datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, si previamente se ha obtenido el consentimiento expreso del afectado[59] y se ha informado a éste de su derecho a no prestarlo. Se exceptúan de este requisito los ficheros propiedad de los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de datos necesita el consentimiento expreso previo del afectado. Los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual, están radicalmente prohibidos (artículo 7.4).

Si los datos hacen referencia al origen racial o étnico[60], a la salud o a la vida sexual del afectado, sólo podrán ser recogidos, tratados y cedidos cuando, por razones de interés general, una ley así lo disponga o el afectado consienta expresamente. En estos supuestos, sólo cabrá un tratamiento cuando éste resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Esta habilitación se completa en el artículo 8, ya que se habilita a las Instituciones, centros sanitarios públicos y privados y a los profesionales correspondientes, para el tratamiento de datos relativos a la salud de las personas que a aquellos acudan, o hayan de ser tratados en los mismos, de acuerdo con la legislación sanitaria estatal o autonómica[61]. También podrá

[59] Si este tipo de datos se recogen a través de una Web, para que goce el consentimiento expreso de validez ante la APD, en el procedimiento de recogida se deberá articular algún procedimiento que permita al usuario de manera expresa y activa, prestar su consentimiento a que sus datos sean recabados y tratados. Véase Recomendaciones de la APD al sector del comercio electrónico, para la adecuación de su funcionamiento a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

[60] En relación con este tipo de datos, la APD entiende que no pueden considerarse como tales los datos relativos al aspecto externo de las personas, como el color de la piel o la apariencia física. Para que se dé este supuesto, el tratamiento deberá establecerse por motivo de la raza u origen. Para más información, véase APARICIO SALOM, ob. últ. cit., página 204.

realizarse el tratamiento para salvaguardar el interés vital del afectado o de otra persona, si el afectado se encuentra física o jurídicamente incapacitado para dar su consentimiento. Al no estar definidos estos conceptos en la LOPD, se han planteado dudas sobre su alcance y contenido.

La última categoría de datos especialmente protegidos son los relativos a la comisión de infracciones penales o administrativas. En estos supuestos, los datos de carácter personal sólo podrán ser incluidos en los ficheros de la Administraciones Públicas competentes para ello, según las distintas normas reguladoras.

Las cesiones de datos son muy comunes en las actividades de publicidad o marketing directo, existiendo diversas modalidades de contratos, tales como: el arrendamiento de datos por el cual una empresa arrienda los datos que posee a una tercera empresa para que los utilice para una o varias campañas publicitarias, y que en nuestra opinión deberá formalizarse por escrito indicando los usos y finalidades del arrendamiento, así como las obligaciones y límites del arrendatario. Otra modalidad se encuentra en la ejecución de campañas de márketing, por la cual una empresa ofrece a terceros la posibilidad de utilizar los ficheros que posee para la ejecución de la campaña, en este caso la empresa arrendataria debe ser diligente a la hora de elegir a la empresa arrendadora, ya que atendiendo a la doctrina de la APD, la arrendataria es la que ordena el tratamiento y por ende, puede ser sancionada si no se obtuvo el consentimiento por parte de la arrendataria de los interesados a los que se dirija la publicidad, postura refrendada por la Sentencia de la Audiencia Nacional de 21 de junio de 2002, que establece en un caso similar al descrito que el responsable de tratamiento es aquel que decide sobre la finalidad y usos del fichero y del tratamiento, es decir, además del que decide y trata, se entiende responsable al que teniendo poder de decisión encomienda la materialidad del tratamiento a un tercero, lo que sucede cuando se contrata a otra empresa para que realice una campaña publicitaria. La tercera modalidad es la impresión de etiquetas y entrega posterior a la arrendataria, para que las pegue y las envíe. Esta actividad, en lo que se refiere a quién se considera responsable del fichero, no es pacífica, existiendo opiniones contradictorias entre la APD y la jurisprudencia[62]. Por

[61] En este supuesto, deberá tenerse en cuenta la Ley 14/1986 de 25 de abril General de Sanidad. Un completo estudio de la materia se encuentra en APARICIO SALOM, ob. últ. cit., páginas 196 y ss.

[62] Para una análisis más detallado de la cuestión puede verse APARICIO SALOM, ob. últ. cit., páginas 191 y ss.

último se encuentra el alquiler de espacio publicitario. En virtud de este contrato una empresa que envía regularmente documentación a sus clientes, con vistas a amortizar los costes de envío, remite publicidad de terceros. En ese supuesto, debe requerirse el consentimiento del afectado, ya que se produce una desviación de la finalidad de uso de los datos, para la cual el interesado prestó su consentimiento.

Para el tercero al que se comunican los datos, cabe decir que queda sometido, aunque no sea el responsable del fichero, a todas las obligaciones que impone la ley.

Entrando a continuación en el apartado del acceso a los datos por parte de un tercero, comenzaremos distinguiéndola de la comunicación de datos. Para que no se considere comunicación, el acceso ha de ser necesario para la prestación de un servicio al responsable del fichero. Este acceso para ser legal ha de constar por escrito o de alguna manera que permita hacer constar su celebración y contenido en un contrato, estableciéndose expresamente que ese tercero, denominado encargado de tratamiento[63], únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en el contrato, ni los comunicará, ni siquiera para su conservación a otras personas, en cuyo caso sería considerado a todos los efectos como responsable del fichero. En el contrato se estipularán las medidas de seguridad que correspondan al fichero en cuestión, que el encargado de tratamiento está obligado a poner en práctica. Una vez finalizada la relación contractual, el encargado de tratamiento viene obligado a la devolución o destrucción de los datos de carácter personal que posea.

Debemos manifestar que en lo que respecta a los derechos de acceso, rectificación y cancelación, además de la normativa recogida en la LOPD, debemos acudir al Real Decreto 1332/1994 de 20 de junio, por el que se desarrollan diversos aspectos de la ley orgánica (reglamento LORTAD) y a la Instrucción de la APD 1/1998 de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. Ambos fueron promulgados bajo la vigencia de la LORTAD, pero en virtud de la disposición transitoria tercera de la LOPD, se encuentran vigentes.

Se trata de derechos personalísimos, es decir, que, en principio, sólo pueden

[63] La definición que le otorga el artículo 3 g) de la LOPD, es la siguiente: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

ser ejercitados por el titular del derecho, salvo que se encuentre en situación legal de incapacidad o minoría de edad, en cuyo caso podrán ser ejercitados por su representante legal. No obstante, la APD en su Memoria de 2001, página 311, se manifestó favorable a que pueda ejercerse el derecho por parte de una persona distinta del titular, siempre que exista un poder o mandato, que no podrá ser genérico, sino que debe referirse concretamente al ejercicio de uno de esos derechos.

Al estar considerados como derechos independientes, se entiende que es el titular el que elige cual ejercita, no estando subordinado el ejercicio de alguno de estos al ejercicio anterior de ninguno de los mismos. Para poder ser ejercitado deberá remitirse al responsable del fichero una comunicación que debe contener los siguientes extremos: nombre y apellidos del interesado y fotocopia de su DNI (o cualquier otro medio que acredite la identidad, que sea válido en derecho). Si se trata de representante legal deberá adjuntarse igualmente su fotocopia del DNI y copia del documento acreditativo de la representación. Deberá igualmente incluirse la petición en la que se concreta la solicitud, designar un domicilio a efectos de notificaciones, fecha y firma del solicitante y en su caso, documentos en los que se acredita la solicitud. El método de envío de la solicitud deberá acreditar el envío y la recepción. El responsable del fichero viene obligado a cursar la solicitud, aunque no posea datos de carácter personal del solicitante, debiendo utilizar de la misma manera un método que acredite el envío y la recepción.

4.6. DERECHO A IMPUGNAR VALORACIONES

Siguiendo los derechos de las personas, pasamos a continuación a estudiar el derecho de impugnación de valoraciones. En virtud de este derecho, los ciudadanos no podrán verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. De la misma manera, podrán impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fin sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad, teniendo derecho a obtener del responsable del fichero información sobre los criterios de valoración y el programa utilizado a tales efectos. En este supuesto, pueden plantearse dudas si en

el tratamiento de datos personales se utiliza la actividad de almacenamiento de datos o *datawarehousing*. En mérito a esta actividad, el responsable del fichero almacena todo tipo de información relativa a una persona, incluso la que en principio no es relevante para el uso y finalidad del tratamiento, para después emitir las correspondientes conclusiones de perfil psicológico y sociológico del afectado.

4.7 DERECHO DE INDEMNIZACIÓN

El último derecho reconocido a las personas es el derecho de indemnización. En virtud del mismo, los interesados que a consecuencia de incumplimientos de las disposiciones de la LOPD, por parte del responsable o del encargado del tratamiento, sufran daño o lesión en sus bienes y derechos, tendrán derecho a solicitar una indemnización[64].

5. INFRACCIONES Y SANCIONES

Como en cualquier ley en la que se establecen derechos y obligaciones para las partes, la LOPD incluye una serie de **sanciones** para disuadir a los responsables y encargados del tratamiento, de las tentaciones de actuar en contra de lo establecido legalmente. La LOPD no ha tipificado ningún delito, sino que se remite a la jurisdicción penal y civil. Así pues, quien se crea perjudicado en sus intereses por una actuación ilícita en el ámbito de la protección de datos de carácter personal y pueda demostrar que se le ha causado un daño podrá presentar la correspondiente demanda ante la jurisdicción civil solicitando una indemnización por daños y perjuicios. De igual forma, la vulneración del derecho a la intimidad en sus aspectos más graves se remite a la sede penal y, así, es en el Código Penal donde se recogen este tipo de delitos[65].

La LOPD sujeta a los responsables del fichero y a los encargados del tratamiento al régimen sancionador establecido en el Título VII de la misma. El

[64] Esta indemnización deberá solicitarse ante la jurisdicción ordinaria, en caso de tratarse de ficheros de titularidad privada, o de acuerdo con la legislación reguladora de la responsabilidad de las Administraciones Públicas, en el caso de que nos encontremos ante un fichero de titularidad pública. La indemnización, al no disponer la ley otra cosa, vendrá determinada por la responsabilidad que establece nuestro derecho. En caso de que entre el afectado y el responsable o encargado de tratamiento medie una relación contractual, la responsabilidad se entenderá contractual. En el caso de que no exista tal relación, la indemnización traerá causa de la responsabilidad extracontractual o Aquiliana, del artículo 1.902 del Código Civil.

artículo 44 de la citada Ley establece las conductas que son consideradas como **infracción,** en los siguientes términos:

1) Según el artículo 44,2 de la LOPD, son infracciones leves las siguientes:

a) "No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda". Se infringe en este caso el artículo 16 de la LOPD que obliga al responsable del tratamiento a hacer efectivo este derecho en el plazo de diez días.

b) "No proporcionar la información que solicita la APD en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con los aspectos no sustantivos de la protección de datos". Es función de la Agencia de Protección de Datos, según establece el artículo 37, i) de la LOPD, recabar de los responsables de los ficheros o de los tratamientos cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

c) "No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave". Según el artículo 26 de la LOPD, "toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo debe notificar previamente a la Agencia de Protección de Datos".

d) "Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente ley". Según el artículo 5 de la LOPD los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de una serie de circunstancias sobre el fichero, previéndose en dicho artículo una serie de excepciones.

e) "Incumplir el deber de secreto establecido en el artículo 10 de esta ley, salvo que constituya infracción grave". El artículo 10 de la LOPD obliga al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del fichero.

2) Infracciones graves, según el artículo 44,3 de la LOPD, son las siguientes:

a) "Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de dis-

[65] El Título X de nuestro Código Penal está dedicado a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Ver, por ejemplo, el artículo 197,2º.

posición general, publicada en el BOE o diario oficial correspondiente". Según el artículo 20 de la LOPD, "la creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente".

b) "Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad". Uno de los principios en que se inspira la LOPD es el de finalidad por el que, como establece el art. 4,1 de la LOPD, "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

c) "Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible". El artículo 6 de la LOPD ordena, salvo en una serie de casos que figuran como excepciones, recabar el consentimiento inequívoco como trámite previo al tratamiento de los datos de carácter personal.

d) "Tratar los datos de carácter personal o usarlos posteriormente con conculcación de principios y garantías establecidos en la presente ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave". Se trate de un precepto de carácter muy general referido a la fase de tratamiento de los datos.

e) "El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada". El artículo 15 de la LOPD otorga al afectado la posibilidad de solicitar y obtener información sobre datos de carácter personal que figuren en los ficheros; asimismo, según el artículo 30 de la LOPD, tendrán derecho a oponerse al tratamiento de sus datos con fines de publicidad y de prospección comercial.

f) "Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan, cuando resulten afectados los derechos de las personas que la presente ley ampara". Según el artículo 16 de la LOPD, "el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días".

g) "La vulneración del deber de guardar secreto sobre los datos de carácter

personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad el individuo".

h) "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen". La seguridad en general a la que se refiere el artículo 9 de la LOPD es uno de los pilares sobre los que se ha de cimentar la protección que otorga la Ley, pues sin ella prácticamente nada se puede garantizar.

i) "No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos". La Agencia de Protección de Datos tienen entre sus funciones, según establece el artículo 37, i) de la LOPD, la de "recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones".

j) "La obstrucción al ejercicio de la función inspectora". Una de las potestades que la Ley concede al Director de la Agencia de Protección de Datos es la potestad inspectora. Así, como establece el artículo 40 de la LOPD, "las autoridades de control podrán inspeccionar los ficheros que contengan datos de carácter personal recabando cuantas informaciones precisen para el cumplimiento de sus cometidos".

k) "No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la APD". Una de las potestades que la Ley concede al Director de la Agencia de Protección de Datos es la potestad inspectora. Así, como establece el artículo 40 de la LOPD, "las autoridades de control podrán inspeccionar los ficheros que contengan datos de carácter personal recabando cuantas informaciones precisen para el cumplimiento de sus cometidos".

l) "Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta ley, cuando los datos hayan sido recabados de persona distinta del interesado". Según el artículo 5,4 de la LOPD, "cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los

datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo".

3) Según el artículo 44,4 de la LOPD son infracciones muy graves las siguientes:

a) "La recogida de datos en forma engañosa y fraudulenta". El artículo 4,7 de la LOPD prohíbe la recogida de datos cuando ésta se efectúa por medios desleales, fraudulentos o ilícitos.

b) "La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas". La comunicación o cesión de datos a un tercero sin consentimiento del interesado deja a éste indefenso y puede vulnerar lo dispuesto en el artículo 4,2 de la LOPD.

c) "Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7, cuando no medie el consentimiento expreso del afectado, recabar y tratar los datos referidos en el apartado 3 del artículo 7, cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en al apartado 4 del artículo 7". El tratamiento de datos especialmente protegidos, sin las debidas garantías para el afectado, es lógico que sea sancionado con dureza por las especiales características de dichos datos en relación con la intimidad de la persona y el perjuicio que su conocimiento por terceros sin su consentimiento puede suponer.

d) "No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la APD o por las personas titulares del derecho de acceso". Si se efectúa el tratamiento de datos de carácter personal de forma ilegítima, los afectados pueden solicitar del responsable del fichero que cese en ese tratamiento, pudiendo reclamar ante el Director de la Agencia de Protección de Datos en caso de no ser atendidos.

e) "La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcione un nivel de protección equiparable sin autorización del Director de la APD". La transferencia de datos a un país que no garantice unas condiciones mínimas de protección deja al afectado totalmente desprotegido respecto a cómo van a ser utilizados sus datos de carácter personal y con qué finalidad; por ello es necesario tomar toda esta serie de cautelas.

f) "Tratar los datos de carácter personal de forma ilegítima o con menos-

precio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales". La referencia a los derechos fundamentales que aquí hace el legislador parece redundante pues los derechos a los que puede afectar son los que protege precisamente la propia LOPD.

g) "La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas". Se comete una infracción muy grave de las previstas en la LOPD cuando se vulnera el deber de guardar secreto sobre los datos correspondientes a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, así como los datos de carácter personal recabados para fines policiales, siempre y cuando no exista consentimiento de la persona afectada.

h) "No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición". La reiteración en la no atención u obstaculización en el ejercicio de los derechos de acceso, rectificación, cancelación u oposición agrava la infracción que ya figuraba como grave en la propia LOPD.

i) "No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero". La reiteración en la falta de notificación de la inclusión de datos de carácter personal en un fichero agravará la infracción que ya figuraba en la propia LOPD.

La LOPD sólo contempla sanciones administrativas que se conviertan en multas en el caso de los ficheros privados y en propuestas de sanciones disciplinarias en el caso de los ficheros públicos. Estarán sujetos al régimen sancionador establecido en la LOPD los responsables de los ficheros o responsables de los tratamientos y los encargados de los tratamientos. Las sanciones que puede imponer la APD, en el ejercicio de sus funciones se recogen en el artículo 45 de la LOPD y se dividen, tal y como corresponde a las infracciones, en leves, graves y muy graves[66]. Las sanciones son de 601,01 euros a 60.101,21 euros

[66] Según establece el artículo 45,4 de la LOPD, "la cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, el volumen de los tratamientos afectados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora".

para las leves, de 60.101,21 euros a 300.506,05 euros para las graves y, de 300.506,05 euros a 601.012,10 euros para las muy graves. Esta cuantía podrá ser actualizada periódicamente por el Gobierno, de acuerdo con las variaciones experimentadas en los índices de precios.

Además, el artículo 46 de la LOPD regula el procedimiento sancionador en el caso de que las infracciones que señala el artículo 44 se cometan en ficheros de los que sean responsables las Administraciones Públicas[67].

En lo que respecta a la prescripción de las infracciones, debemos estar a lo dispuesto en el artículo 47,1 que dispone que, las infracciones muy graves prescribirán a los tres años, las graves a los dos y las leves lo harán pasado un año. Los mismos periodos se establecen para la prescripción de las sanciones. Este plazo comenzará a computarse desde el día en el que se hubiera cometido la infracción, o desde el día siguiente a aquel en que la resolución que impone la sanción obtenga el carácter de firmeza. Pero como en todo trámite administrativo, la iniciación del procedimiento sancionador, con conocimiento del interesado, interrumpirá estos plazos. No obstante, si el expediente estuviera paralizado durante más de 6 meses por causas no imputables al presunto infractor, se reanudará este plazo. Si se trata de una sanción, la prescripción la interrumpirá la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a correr el plazo si este procedimiento se encuentra paralizado durante más de 6 meses, por causa no imputable al infractor.

Este procedimiento se configura como un procedimiento sancionador administrativo tipo, y sus pasos se encuentran minuciosamente regulados en el artículo 18 y 19 del Real Decreto. Añadiremos que para todo lo no previsto en estos artículos, regirá el procedimiento general del ejercicio de la potestad sancionadora previsto en el R. D. 1398/1993 de 4 de agosto, que regula el

[67] Ante una infracción de este tipo, el Director de la APD dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. Según establece el artículo 46,2 de la LOPD, "el Director de la Agencia de Protección de Datos podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran" y, "el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas".Además, "se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieran los apartados anteriores", según señala el artículo 46,3 de la LOPD. Según el artículo 46,4 de la LOPD, "el Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

Procedimiento para el Ejercicio de la Potestad Sancionadora, en desarrollo de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

El artículo 48 de la LOPD establece que el procedimiento sancionador se establecerá por vía reglamentaria, correspondiendo a la APD la competencia sobre el mismo. En la medida en que no existe desarrollo reglamentario posterior a la entrada en vigor de la LOPD, la misma establece en su Disposición transitoria tercera la vigencia del Real Decreto 1332/1994 de desarrollo de la LORTAD.

El procedimiento sancionador se iniciará mediante acuerdo de la APD. Siempre de oficio, por propia iniciativa o bien por denuncia de cualquier persona afectada por la conducta del responsable del fichero. En dicho acuerdo la APD designará un instructor[68] y un secretario, identificándose a la persona o personas presuntamente responsables con concreción de los hechos que se le imputen, infracción a la que dan lugar y sanción que le corresponda, pudiendo incluirse en la misma, la adopción de medidas provisionales.

Dentro de los quince días siguientes a la notificación del acuerdo de incoación del expediente, el instructor ordenará de oficio la práctica de cuantas pruebas y actos de instrucción sean adecuados para esclarecer los hechos y determinar las responsabilidades susceptibles de sanción. En idéntico plazo, el presunto responsable podrá formular las alegaciones y proponer pruebas que considere convenientes.

Transcurrido este último plazo, el instructor acordará la práctica de las pruebas que estime pertinentes, a cuyo efecto concederá un plazo de treinta días, transcurrido el cual el expediente se pondrá a disposición del presunto responsable para que, en el plazo de quince días, formule nuevas alegaciones y aporte la documentación que estime de interés en su defensa.

Finalizada la función instructora, el instructor formulará propuesta de resolución en la que se incluirá la infracción y sanción a imponer en cuantía de acuerdo a los criterios marcados en al LOPD, notificándola al presunto responsable para que en el plazo de 15 días pueda formular nuevas alegaciones si lo estima oportuno. Finalizado este plazo, la propuesta y el expediente se

[68] La función instructora compete a la Inspección de Datos, órgano de la Agencia de Protección de Datos, al cual se atribuyen las funciones de inspección de acuerdo con los artículos 27 y ss. del Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la Agencia de Protección de Datos.

elevarán al Director de la Agencia de Protección de Datos que, antes de dictar resolución, podrá proponer que se lleven a cabo cuantas actuaciones considere necesarias en el plazo de quince días. En los diez días siguientes a la expiración de este último plazo el Director de la Agencia de Protección de Datos dictará resolución precisando los hechos imputados, la infracción cometida y precepto en el que se incluye, el responsable de la misma y la sanción impuesta, además de las medidas provisionales que considere oportunas. Esta resolución agota la vía administrativa y contra la misma se podrá interponer recurso contencioso-administrativo.

Además, según se establece en el artículo 49 de la LOPD, "en los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos".

En este sentido, como establece el citado artículo 49 de la LOPD, "si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas".

6. CONSIDERACIONES GENERALES SOBRE TRATAMIENTOS DE DATOS EFECTUADOS A TRAVÉS DE INTERNET

6.1. CONSIDERACIONES GENERALES

Además de las consideraciones apuntadas en los epígrafes anteriores, a fin de completar el análisis sobre la protección de datos, no debemos olvidar que el tratamiento realizado por las entidades que operan a través de Internet[69] presenta una serie de rasgos característicos para el cumplimiento de la normativa sobre protección de datos de carácter personal que se refieren a la información del afectado y al consentimiento y la forma de prestarlo.

En Internet, el deber de información que corresponde al fichero se manifiesta por medio de la política de privacidad que se debe de incluir en un lugar

visible del sitio web. En dicha política de privacidad, el responsable del fichero deberá, cumpliendo con lo previsto en el artículo 5 de la LOPD, informar a los afectados a los que se soliciten datos de carácter personal de modo expreso, previo e inequívoco de las siguientes cuestiones: de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En la práctica, la gran mayoría de los sitios *web* incluyen una dirección de correo electrónico específica para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, aunque esto nos plantea problemas de aplicación en Internet, ya que la APD en la Instrucción 1/1998, de 19 de enero, estableció como necesario, a los fines de poder constatar la identidad de la persona que solicita el acceso a sus datos, el que aporte o remita una copia del D. N. I.

Por otro lado, el responsable del fichero debería dejar constancia en su política de privacidad de su política en cuanto a la cesión o no de los datos a terceras personas y de la solicitud del afectado de su consentimiento para tal menester, de la destrucción de los datos almacenados para el caso de la extinción de la entidad responsable del fichero, de las cláusulas que aclaren como debe realizar el afectado la prestación de su consentimiento para la recogida de sus datos de carácter personal, del uso de mecanismos complementarios de recogida de datos e información de sus visitas, como, por ejemplo, puede ser la efectuada por medio de las cookies, de las cláusulas eximentes de responsabilidad por el tratamiento de datos que efectúen otros sitios webs a las que pueda acceder desde la del responsable del fichero al cliquear sobre un *link*[70], un *banner*[71] o sobre cualquier otro enlace ubicado en la *web* con esta finalidad, de las cláusulas que determinen el plazo de vigencia de la política de privacidad y de la forma en

[69] ÁLVAREZ CIVANTOS, O. J., *Normas para la implantación de un eficaz protección de datos de carácter personal en empresas y entidades,* Ed. Comares, Granada, 2001, pp. 230 y ss.

[70] Hiperenlace (también llamado enlace, vínculo, hipervínculo o liga) es un elemento de un documento electrónico que hace referencia a otro recurso, por ejemplo, otro documento o un punto específico del mismo o de otro documento. Combinado con una red de datos y un protocolo de acceso, un hiperenlace permite acceder al recurso referenciado en diferentes formas, como *visitarlo* con un agente de navegación, mostrarlo como parte del documento referenciador

que se habrá de producir y comunicar el cambio de la misma, de la mención de los derechos de los menores en el tratamiento de sus datos de carácter personal y de la necesidad de que el consentimiento para que el mismo sea concedido por sus padres o tutores.

6.2. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y EL USO DE COOKIES

La defensa del derecho a la intimidad frente al uso de las nuevas tecnologías encuentra su mayor razón de ser en Internet y, en concreto, con el uso de las denominadas *cookies.* La función de estos archivos es la de registrar las visitas que el usuario hace a un determinado sitio *web*[72].

La función básica de las cookies consiste en permitirle a un servidor alma-

o guardarlo localmente. Los hiperenlaces son parte fundamental de la arquitectura de la World Wide Web, pero el concepto no se limita al HTML o a la Web. Casi cualquier medio electrónico puede emplear alguna forma de hiperenlace.

[71] Un *banner* es un formato publicitario en Internet. Esta forma de publicidad online consiste en incluir una pieza publicitaria dentro de una página web. Prácticamente en la totalidad de los casos, su objetivo es atraer tráfico hacia el sitio web del anunciante que paga por su inclusión. Los banners se crean a partir de imágenes (GIF o JPEG), o de animaciones creadas a partir de tecnologías como Java, Adobe Shockwave y, fundamentalmente, Flash, diseñadas con la intención de atraer la atención, resultar notorias y comunicar el mensaje deseado. Por lo tanto, estos banners no necesariamente mantienen la línea gráfica del sitio. Todo tipo de sitios web son susceptibles de incluir toda clase de banners y otros formatos publicitarios, aunque en la mayoría de los casos, son los sitios con contenidos de mayor interés o con grandes volúmenes de tráfico los que atraen las mayores inversiones de los anunciantes. Cada vez que un usuario accede a una página web concreta en la que se ha previsto la inclusión de un banner, éste es mostrado. Esto se conoce como "impresión". En los formatos habituales, cuando el usuario clica sobre el banner, automáticamente es redirigido a otro sitio web, decidido por el anunciante, lo que se conoce como "click through". Cuando se pone el *click through* en relación con las impresiones se obtiene una tasa denominada ratio de *click through* (CTR en sus siglas en inglés) que mide el número de veces que alguien ha hecho click sobre el banner en relación al número de veces que se ha mostrado dicho banner -número total de impresiones-. Esta tasa puede variar muchísimo en función de cada campaña de publicidad pero se puede considerar situada en términos normales si ronda entre el 0,1% y el 1%. Habitualmente, el CTR es el principal indicador que se emplea para medir la eficacia de una campaña de publicidad online. En ocasiones sirve también para determinar el coste que el anunciante pagará por la campaña, aunque fundamentalmente este coste viene determinado por el número de impresiones. El formato clásico de banner es horizontal y mide 468x60 píxeles, aunque existen muchos otros formatos en función del soporte -el sitio web que los acoge-. De hecho, comúnmente el término banner se emplea para referirse a todo tipo de formatos publicitarios online, aunque existen piezas de muy diferentes características.

cenar y más adelante recuperar una pequeña cantidad de información en el ordenador del usuario. Estos datos siempre estarán asociados a un sitio *web* y a un navegador concreto, lo que implica que una *cookie* creada por un servidos en un momento dado sólo le será accesible en el futuro si el visitante regresa a ese sitio *web* usando el mismo ordenador y el mismo navegador. La información es guardada en un archivo de texto, conteniendo sólo aquellos datos que la aplicación servidora expresamente determine. Aunque puede incluir alguna información personal, como códigos de usuario o contraseñas, lo normal es recoger sólo aquellos datos que permitan recordar lo que el usuario hizo en esa ocasión. En el momento en que el usuario en cuestión regresa a ese sitio *web* en cuestión, su navegador envía el contenido de la *cookie* al servidor, que puede entonces interpretarlo y usarlo de modo preestablecido, para, por ejemplo, mostrar un saludo personalizado al usuario.

Frente al uso de las cookies, es cierto que se han diseñado programas anti-*cookies* e incluso la mayoría de los navegadores permiten al usuario elegir una opción que impedirá el almacenamiento de *cookies* en su ordenador pero no es menos cierto que existen determinados sitios *web* cuyo acceso es imposible si no se acepta la instalación de las mismas en el disco duro del ordenador que accede a un determinado sitio *web.*

Ahora bien, en relación con la defensa del derecho a la intimidad y la protección de datos de carácter personal y el uso de las *cookies,* debemos hacer algunas precisiones.

Las *cookies* no pueden capturar información personal de un usuario que no esté dispuesto a cederla voluntariamente. Tampoco pueden transmitir un virus informático porque no contienen más que un texto estático ni entrar en el disco duro del ordenador del usuario y extraer documentos u otros archivos. Hay que tener siempre en cuenta que la utilización de esta técnica no vulnerará el derecho a la intimidad, el derecho a la protección de datos y, por ende, la LOPD, cuando se haga con el consentimiento del usuario.

[72] Si una misma empresa se encarga de transferir cookies a los visitantes de los sitios web, ésta puede recoger una valiosa información acerca de qué sitios web son más visitados por ese usuario, permitiéndole crear perfiles de los usuarios de la red.

La *Revista de Estudios Económicos y Empresariales* recibió este artículo el 31 de julio de 2013 y fue aceptado para su publicación el 11 de septiembre de 2013.