ALGUNAS CUESTIONES EN TORNO AL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS EN LA DENOMINADA «INFORMÁTICA UBICUA»

SOME QUESTIONS ABOUT THE FUNDAMENTAL RIGHT TO DATA PROTECTION IN THE UBIQUITOUS COMPUTING

Juana María Domaica Maroto

Profesora Colaboradora del Departamento de Métodos Cuantitativos e Informáticos
Facultad de CC. Económicas y Empresariales
Universidad San Pablo CEU
domaica@ceu.es

Resumen: Hoy los lugares y formas de captación y tratamiento posterior de datos, sean éstos personales o no, se han multiplicado y una forma global de procesar esos datos en la Red, Internet, ha permitido la irrupción del denominado *ubiquitous computing*.

La ubicuidad de los tratamientos y servicios informáticos en la Red tiene un pilar fundamental en el concepto de *cloud computing*. Este concepto se ha desarrollado al residenciar la información personal y corporativa en la Red, en la «nube» y no únicamente en equipos locales. Por ello, partiendo de este fenómeno imparable de externalización informativa surge el concepto de «informática ubicua. Con un dispositivo y servicios adecuados de acceso a la Red se puede tratar la información y, en concreto, los datos personales desde cualquier área geográfica. La «informática ubicua» abre enormes interrogantes jurídicos.

Abstract: *Today the places and ways of capturing and further processing of data, whether personal or not, have multiplied and a holistic approach to process that data on the Web, Internet, has allowed the emergence of ubiquitous computing called.*

The ubiquity of the treatments and services in the network computer is a cornerstone in the concept of cloud computing. This concept has been developed to impeachment personal and corporate information on the Web, in the «cloud» and not only on local. Thus, from this informative outsourcing unstoppable phenomenon arises the concept of «ubiquitous computing». With a device and adequate access to the network can process information and, in particular, personal data from any geographical area. The «ubiquitous computing opens up huge legal questions.

Palabras clave: Protección de Datos Personales. Externalización de datos. Cloud computing. Informática ubicua.

Keywords: *Personal Data Protection. Outsourcing data. Cloud computing. Ubiquitous Computing.*

Recepción original: 21/08/2012
Aceptación original: 24/08/2012

I. INTRODUCCIÓN

Vivimos en la «sociedad de la información» y en ella se han de desenvolver y ha de ejercitar el individuo sus derechos y, en concreto, el derecho fundamental a la protección de datos.

En la actualidad lo único que se necesita es un dispositivo, que puede ser desde un ordenador portátil hasta un *smartphone* o un *iPad*, y una conexión a Internet para acceder a una amplia variedad de servicios donde se tratan y almacenan datos personales. Así mismo, hoy cualquier persona en cuanto usuario de un teléfono móvil, de una simple tarjeta de fidelización o una tarjeta inteligente es por ello portador de medios de gestión de identidad en un mundo de relaciones M2M (*Machine to Machine*). Aquí se produce la activación automática de conexiones entre dispositivos terminales y un sistema de información que no ofrecen al individuo la posibilidad ni de conocer la existencia del tratamiento de datos personales ni, menos aun, los medios para controlarlo.

Por todo ello, hoy más que nunca los derechos fundamentales del individuo, y en concreto el derecho fundamental a la protección de datos, se erigen en baluartes de su dignidad como persona. Así, considerando estos nuevos entornos, queremos acercarnos a un inicial análisis de las condiciones, dificultades y riesgos que surgen para el ejercicio del derecho de todo individuo a poder disponer y controlar el uso de sus datos personales. Este derecho se traduce en la facultad de dicho individuo para decidir cuáles de esos datos proporcionar a un tercero y también saber quién y para qué los posee, pudiendo oponerse a esta posesión o uso. Ahora bien este derecho a la protección de datos personales, con las facultades que de él dimanan para los titulares de los datos, ha de ser ejercitado actualmente en un entorno digital universal, global. Por ello consideramos necesario aproximarnos al concepto de la sociedad de la información que hoy no se entiende sin Internet.

II. LOS ENTORNOS DE INFORMÁTICA UBICUA Y DE SERVICIOS TIC EN LA *CLOUD*

Ya en el año 1973 el sociólogo estadounidense Daniel Bell introdujo el concepto de «sociedad de la información» en su libro *El advenimiento de la sociedad postindustrial*[1]. En opinión de Bell la base fundamental de esta sociedad sería el conocimiento teórico y, a su vez, los servicios sobre el conocimiento serían la base de la nueva economía.

Unos años después, en 1987, el profesor Romeo Casabona[2], con magistral claridad, expuso que si bien «la revolución industrial del siglo XIX permitió sustituir de forma sustancial el trabajo físico del hombre por máquinas, en la presente centuria estamos presenciando el diseño de otra gran transformación radical: reemplazar determinadas funciones intelectuales del hombre gracias a estas nuevas tecnologías. Esta situación nos está llevando a los inicios de una nueva era: la de la información y la comunicación, en el seno de lo que se ha venido a denominar la sociedad de la información».

En este mismo sentido Manuel Castells[3] afirma que el sistema económico actual todavía se basa en el capitalismo, aunque ya no indus-

[1] BELL, D. *The coming of post-industrial society; a venture in social forecasting,* New York: Basic Books 1973. – xiii, 507.

[2] ROMEO CASABONA, C.M. *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información,* Madrid: FUNDESCO. Colección Impactos, 1987, pág. 15.

[3] CASTELLS, M. *L´etá dell´informazione economica societá cultura,* Milano: Universitá Bocconi, 2004, pág. 130.

trial sino «informacional. Ya hoy cabe hablar de una nueva economía donde el conocimiento y la información son la base de la productividad y la competitividad[4]. Para este autor la nueva economía tiene tres características interrelacionadas: la primera, el conocimiento y la información como base de la productividad y la competitividad y el fortalecimiento de éstas últimas por las tecnologías. Segunda, la nueva economía es una economía en la que el conocimiento y la información se comparten en red y es tecnológicamente simple formar parte de la red, o quedar excluido de la misma, en función de la contribución a la cadena de valor estructurada de información y conocimiento que se genera en dichas redes. Y tercera, añadida a las dos anteriores características, las telecomunicaciones permiten que la economía funcione como una unidad en tiempo real y a escala planetaria. Todo ello está impulsado por una red mundial como Internet que permite la interconectividad de las redes. Así, el Profesor Castells desde un punto de vista económico establece los tres pilares definitorios de la sociedad de la información: información y conocimiento compartidos en redes interconectadas.

Los autores citados desde distintas perspectivas, sociológica, económica, jurídica han planteado con acierto el fundamento de la sociedad actual: la información, los servicios sobre la información que generan conocimiento y su intercambio a través de redes de comunicación, todo ello propiciado por el desarrollo tecnológico.

En la Unión Europea en mayo de 1994 el ministro de Industria alemán, Martin Bangemann, dirigió un grupo de trabajo cuyo objetivo era sentar las bases para alcanzar la sociedad de la información real para todos los ciudadanos. Este grupo, denominado grupo Bangemann, fue el que por primera vez utilizó el término sociedad de la información en el ámbito de la Unión Europea, en su informe denominado informe Bangemann[5].

[4] CASTELLS, M. «Tecnologías de la información y desarrollo global», *Revista Política Exterior*. Vol. XIV. Noviembre/Diciembre 2000, número 78, págs. 151 y ss.

[5] *Europa y la sociedad global de la información*. Recomendación del Grupo Bangemann al Consejo Europeo, 26 de mayo de 1994. Este informe recoge una serie de actuaciones imprescindibles para alcanzar la sociedad de la información que se pueden concretar resumidamente en cinco puntos: 1. actuación conjunta de todos los Estados miembros con concienciación de la ciudadanía y de los poderes públicos y privados; 2.evitar una fractura de la sociedad en dos niveles teniendo solo uno de ellos acceso real a los beneficios y posibilidades de la sociedad de la información; 3. fomento de la competencia entre los operadores de telecomunicaciones y titulares de los medios de comunicación; 4. imprescindible fomento de la estandarización de los sistemas, interconexión de las redes telemáticas y la interoperabilidad de los servicios y las aplicaciones y por último y fundamental. 5. protección de los derechos de propiedad intelectual y el derecho a la intimidad de los individuos a través de la regulación de la protección del dato de carácter personal.

Más recientemente un concepto amplio de sociedad de la información se recoge en la exposición de motivos de la Ley española de Servicios de la Sociedad de la Información. Este concepto amplio viene determinado «*(…) por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información*[6].

Efectivamente el concepto de sociedad de la información nace y está ineludiblemente unido al concepto de red de telecomunicación, red de telecomunicación que lleva de suyo la presencia de medios informáticos interconectados[7]. Así la red global por excelencia, la red de redes, Internet, ha contribuido a debilitar las antiguas barreas de tiempo y espacio que, sin que fueran absolutamente infranqueables, guardaban algunos de nuestros derechos individuales, e indudablemente, entre otros, nuestra privacidad. Así la telemática puede constituir, como ya adelantó el profesor Romeo Casabona[8], «el cauce potencial para una intromisión no deseable en la intimidad individual». Y, a continuación, se hacía una pregunta que adquiere hoy una relevancia innegable «¿Estamos en camino de pasar a convertirnos en ciudadanos transparentes, a modo de escaparates de uno de los aspectos más preciados de nuestra personalidad?» Cabría calificar de premonitoria y de plena actualidad la pregunta y el término de «ciudadanos transparentes»[9].

---

[6] Ley 34/2002, de 11 de julio. BOE 12 julio 2002, núm. 166, [pág. 25388]; rect. BOE 6 agosto 2002, núm. 187, [pág. 28951.

[7] En este mismo sentido Campuzano Tomé entiende que es el desarrollo y la universalización de las nuevas tecnologías de la información y las comunicaciones las que tendrán un impacto calificable de revolución en el ámbito cultural, económico, legal y social. H. Campuzano Tomé, *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información,* Madrid: Tecnos, 2000, pág. 19.

[8] ROMEO CASABONA, C.M. Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información, cit., pág. 16.

[9] Este concepto de «ciudadanos transparentes» puede adquirir nuevo significado con la extensión del uso de la tecnología biométrica (software y hardware) que puede llegar a extraer, leer, del interior del cuerpo humano lo más oculto y profundo: desde la presión arterial, la frecuencia de latidos del corazón, el fondo de ojo, etc. Hoy conocemos la tecnología aplicada al control de acceso a determinadas zonas de embarque en algunos aeropuertos donde se aplican escáneres corporales a los pasajeros en un ejercicio de auténtica transparencia corporal. Ya la Exposición de Motivos de la LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal) nos advertía que el tiempo y el espacio habían sido barreras que en el pasado preservaron nuestra intimidad y ahora, cabría añadir, también en el pasado nuestro cuerpo encerraba dentro de sus límites la información que a él le concernía. Hoy la tecnología biométrica traspasa ese límite y hace posible la exposición y manifestación pública de la información de la identidad del individuo. Posiciones a favor y en contra de la implantación de sistemas de reconocimiento biométrico pueden manifestarse al respecto. Un sistema biométrico puede

Esta conectividad de redes ha llegado a tener un carácter mundial gracias al desarrollo de Internet que para el Libro Verde sobre la convergencia de los sectores de las telecomunicaciones «puede considerarse una red de redes interconectadas de forma abierta mediante IP, que normalmente se vale de enlaces de transmisión alquilados a los operadores de telecomunicaciones. […] El carácter abierto, sin pertenencia a un propietario, de las normas de Internet ha hecho posible que las empresas puedan aprovechar y dar continuidad a los avances realizados por otras empresas del sector»[10].

Sin dejar de lado todo lo expuesto el paso fundamental que ha permitido la evolución de los servicios web en la Red es el desarrollo de una plataforma universal de interacción online personalizada. Hoy la Red permite establecer a los individuos una interacción personalizada y un reconocimiento personal remoto. Aquí radica uno de los cambios sustantivos que ha supuesto Internet al permitir la interrelación entre personas identificadas atribuyéndoles efectos jurídicos a su actuación. La extensión o expansión mundial de la Red ha conducido a una casi ubicuidad en el reconocimiento e interacción personalizada en el entorno global.

Así, con el planteamiento expuesto, hoy los lugares y formas de captación de datos, sean éstos personales o no, se han multiplicado y lo que es aún más relevante una forma global de procesar esos datos en la Red, Internet, ha permitido la irrupción de la denominada «computación ubicua»[11]. La informática ubicua se ha hecho posible porque existe una red mundial como Internet donde se puede ga-

constituirse en un medio adecuado de autenticación en el sentido de verificación o control de acceso a lugares públicos y/o privados. Y, así mismo, puede ser, un medio de identificación de personas. Desde una perspectiva criminológica la utilización de sistemas biométricos puede aportar un medio valioso de lucha contra la delincuencia. Pero también posiciones escépticas plantean los riesgos que para los derechos individuales y para la propia estructura democrática pueden llegar a representar los sistemas de reconocimiento biométrico.

[10] Junto al carácter abierto de Internet el informe también señala como una de las características fundamentales que han favorecido la conectividad a través de Internet el hecho de la independencia tecnológica de Internet de la plataforma sobre la que se implanta, ya que el protocolo IP se ha convertido en «el protocolo de red de facto de Internet capaz de encaminar y transportar todos los elementos de un servicio multimedios (texto, imagen, vídeo de animación y sonido)». Cfr. Comisión Europea. COM(97) Versión 3. *Libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación, en la perspectiva de la sociedad de la información.* Bruselas, 3 de diciembre de 1997. Pág. 4. Disponible en la página web: http://www.euskalnet.net/oig/archivo/lvmedia.pdf

[11] LAGE, J. «*El cloud computing* no está en la nube», Revista *GEOECONOMÍA*, n.º 4, Invierno 2010-2011, Págs. 60 ss.

rantizar la confidencialidad de la información que se intercambia y la identidad de las personas que intervienen. Sin confidencialidad o sin identificación no hay base para hablar de una informática ubicua porque el simple hecho de que «todo esté conectado con todo» y con un acceso muy simple para el usuario final no pasaría de ser un caos global sin las dos premisas apuntadas. Podríamos, con todo lo expuesto hasta aquí y al menos en una visión parcial del fenómeno, hacer sinónimos sociedad de la información y sociedad-red. Y, sin duda como ya hemos visto, esta sociedad-red es una sociedad global. El ciberespacio, generado por la extensión de Internet, cruza Estados, fronteras nacionales y ordenamientos jurídicos como el aire que nos envuelve.

Con todo ello hemos puesto de manifiesto un aspecto de la sociedad de la información, como sociedad-red globalmente intercomunicada y ubicua, que exige confidencialidad e identificación[12], de lo contrario hablaríamos de la sociedad del caos, la Babel global. Y este requerimiento de identificación, entendido como exigencia de unión o correlación segura entre el dato captado y una identidad que, en abstracto, preexiste a dicha captación, debe presidir todo el proceso de tratamiento de la información personal. Así adquiere una importancia renovada el derecho a la identificación de cada individuo, y por extensión una identificación digital. La vulneración de este derecho a la identificación puede acarrear consecuencias muy graves para derechos fundamentales de la persona tales como el derecho a la libertad y a la seguridad o incluso el derecho a la vida, y en concreto para el derecho a la protección de datos que ahora nos ocupa.

La intercomunicabilidad a nivel global de un modo transparente y simple para el usuario final, junto a la confidencialidad e identificación de los intervinientes en la conexión y la tendencia creciente a considerar que puede resultar más eficiente situar los recursos informáticos (*hardware* y *software*) y procesos fuera del entorno local habitual, externalizando procesos antes solo concebibles en local y ahora residenciados donde sean más económicos, flexibles y prácticos, porque ya no importa el dónde puesto que el tratamiento automatizado de la información ha llegado a ser ubicuo, lleva al planteamiento de un entorno de nube informática global donde, entre otras

[12] En este sentido se puede afirmar que «… vivimos en la sociedad de la identificación permanente, del tratamiento automático de la información personal y de la creación de perfiles». M. R. Llácer Matacás, *Protección de datos personales en la sociedad de la información y la vigilancia,* Madrid: La Ley, 2011, pág. 18.

muchas cuestiones, la supervivencia de los derechos fundamentales de los individuos es imprescindible.

III. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS EN UN ENTORNO DE INFORMÁTICA UBICUA

Aunque pueda resultar una obviedad, con lo que hasta aquí hemos dicho, podemos afirmar que la información es el valor fundamental de la nueva sociedad. El funcionamiento de la sociedad actual se basa en la información y cabría añadir la información de calidad y legítimamente obtenida y tratada. El tratamiento de una información no veraz (obsoleta, sesgada, incompleta, recabada sin consentimiento ni sujeción a la ley)[13] puede acarrear gravísimas consecuencias tanto en la esfera privada como pública para individuos y Estados.

Así también llegamos a vislumbrar la estrecha relación que entre la sociedad de la información y los datos, en general, y los datos personales, en particular, existe ya que la base de aquélla son éstos.

III.1. Breve referencia a la naturaleza y contenido del Derecho Fundamental a la Protección de datos

Los derechos fundamentales como derechos del ámbito jurídico-público, siguiendo al Prof. Sánchez González, protegen «esferas de libertad, de poder hacer, reconocidas a los individuos frente al Estado, o frente al poder político cualquiera que sea su configuración. [14] Por tanto, se plantean los derechos fundamentales como derechos individuales pero aunque este sea su carácter originario no es menos

[13] Ya el profesor Romeo Casabona apuntó cómo los ordenadores son instrumentos de trabajo de especial magnitud y utilidad al reunir cuatro características esenciales: la ingente potencialidad para el almacenamiento de datos; la gran velocidad de sus operaciones; la adaptabilidad a las exigencias humanas y la exactitud y fiabilidad de estas pero puntualizaba el autor «siempre que sean correctos los datos de partida». Evidentemente si tratamos datos corrompidos obtenemos información corrompida. Por ello el mismo autor llama la atención sobre la aparición de un nuevo valor en nuestra sociedad «el valor de la información sobre la información « entendiendo por tal el valor del acceso a la información pertinente y fiable. C.M. Romeo Casabona, *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información, cit.,* pág. 19.

[14] SÁNCHEZ GONZÁLEZ, S. «Dogmática y Práctica de los Derechos Fundamentales», en S. Sánchez González (ed.), *Los derechos fundamentales en la Constitución Española de 1978,* Valencia: Tirant lo Blanch, 2006, págs. 26 y ss.

cierto que en los derechos fundamentales cabe descubrir lo que Sánchez González califica de una naturaleza adicional que se refiere a su dimensión objetiva, «*como elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia […] plasmada en el Estado de Derecho […]. (STC 25/81, F.j. 5)*[15]. De esta naturaleza de los derechos fundamentales como derechos subjetivos pero que, a la vez, tienen un contenido objetivo, al ser principios o valores superiores del ordenamiento jurídico, se derivan consecuencias importantes como son el deber para el Estado de crear condiciones que permitan su ejercicio[16]. Pero como acertadamente expone el Prof. De Vega «la situación de indefensión a que se ve sometido el individuo en una sociedad (y la nuestra lo es), dominada, controlada y dirigida por poderes privados (aunque no sólo por ellos), hace que el planteamiento de los derechos y libertades no se conciba ya sólo en relación al poder del Estado, sino ante ese conjunto de poderes privados capaces también de conculcarlos»[17].

Y es en este contexto en el que nos plantearemos el ejercicio del derecho fundamental a la protección de datos. Parece que hoy la sombra amenazante de un Estado vigilante que se cierne sobre los individuos deja paso a otra amenaza proveniente de los poderes privados. La amenaza vislumbrada por Orwell en su libro «1984 de «el gran hermano» vigilante debe ser contextualizada en un entorno autoritario, no democrático, donde la división de poderes y el control judicial independiente no se contemplan[18]. Sin embargo, hoy en la mayoría de Estados de nuestro entorno el principio de la división de poderes y el control judicial existen. Por tanto, hay que partir de esta idea y avanzar un poco más. Así siguiendo a Nehf, del gran hermano vigilante, del «*Big brother*», hoy cabe hablar que se ha pasado a una multitud de «*Little brothers* de situaciones de la vida cotidiana donde la recogida de datos personales es continua y casi inconsciente y en la que los individuos participan voluntariamente[19].

---

[15] SÁNCHEZ GONZÁLEZ, S. «Dogmática y Práctica de los Derechos Fundamentales», cit., pág. 28.

[16] GALLEGO ANABITARTE, A. Derechos Fundamentales y Garantías Institucionales: Análisis y Doctrina Jurisprudencial, Madrid, Civitas, 1994, págs.. 98 y 99.

[17] DE VEGA GARCÍA, P. «La Crisis de los Derechos Fundamentales en el Estado Social», Derecho y Economía en el Estado Social, Madrid: Tecnos, 1988, pág. 130.

[18] ARZOZ SANTISTEBAN, X. Videovigilancia, seguridad ciudadana y derechos fundamentales, Cizur Menor: Civitas, 2010, pág. 28.

[19] NEHF, J.P. «Recognizing the societal value in Information privacy», 78 Wash. L. Rev. 1 2003, págs. 11 ss. Abundando en esta idea cabe decir que se trata de un estado de la situación más común en el ámbito privado que en el público y que algunos autores han bautizado con el término de «Internet of things», es decir, un intercambio y una interrogación on line en actos de la vida cotidiana como el consumo, uso

Abundando en esta idea, en opinión de Llácer[20], este estado de la situación es más frecuente en el ámbito privado que en el público y puede denominarse «*Internet of things*», es decir, un intercambio y una interrogación constante, rápida y *on line* en actos de la vida cotidiana como el consumo, uso de la sanidad, acceso a edificios que generan una multitud de puntos de suministro de datos personales que dentro de una red global como Internet, con las facilidades de intercambio que conlleva, puede restar iniciativa, proactividad, en el intercambio de datos a las personas y trasladarla a las cosas. Así se podría incluso hablar de una cosificación de los individuos que llega a su exponente más evidente con los sistemas de implantación en el cuerpo humano de dispositivos electrónicos, por ejemplo, de geolocalización para personas enfermas, o personas sometidas a una medida cautelar judicial.

Es en este nuevo panorama donde el individuo ha de ejercitar su derecho fundamental a la protección de datos.

Muy brevemente es necesario recordar el momento a partir del cual se puede hablar del reconocimiento del derecho fundamental a la protección de datos como derecho independiente que es el año 2000. En ese año 2000, coincidiendo en Europa con la proclamación de la Carta de los Derechos Fundamentales de la Unión Europea, en España el Tribunal Constitucional dicta dos importantísimas sentencias: la 290/2000 y la 292/2000. A partir de este momento sin duda cabe considerar la protección de datos de carácter personal como un verdadero Derecho fundamental autónomo e independiente del Derecho a la intimidad. Así el artículo 8 de la citada Carta dispone: «*Toda persona tiene Derecho a la protección de los datos de carácter personal que la conciernan*»[21]. Como expone con extrema claridad

de la sanidad, acceso a edificios que generan una multitud de puntos de suministro de datos personales que dentro de una red global como Internet con las facilidades de intercambio que conlleva puede restar iniciativa en el intercambio de datos a las personas y trasladarla a las cosas.

[20] LLÁCER MATACÁS, M.R. «La autodeterminación informativa en la sociedad de la vigilancia: Ubiquitous Computing», en M.R. Llácer Matacás (ed.), Protección de Datos Personales en la Sociedad de la Información y la Vigilancia, Madrid: LA LEY, 2011, págs. 66 ss.

[21] En este análisis *ius* fundamental podremos comprobar cómo del principio de legalidad, en su formulación decimonónica original donde partiendo del planteamiento de Rousseau de que la ley es expresión de la voluntad general y la protección de la libertad individual se produce por la ley, se tiende a sustituir por un principio de constitucionalidad donde las libertades individuales deben ser protegidas frente a la ley. La ley entendida como ley ordinaria sometida a las contingencias y vaivenes políticos. Así adquiere la Constitución el papel de pilar y salvaguarda de los derechos y libertades fundamentales de un país o de un conjunto de países y en nuestro entor-

el Prof. Piñar Mañas[22] partiendo del Derecho a la intimidad y privacidad, pasando por el llamado Derecho a la autodeterminación informática o informativa, se ha llegado al reconocimiento como derecho independiente del Derecho a la protección de datos. Por ser muy ilustrativo del contenido de este derecho fundamental a la protección de datos reproducimos el Fundamento Jurídico Séptimo de la Sentencia del TC 292/2000:

«7. … el contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese Derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional el Derecho fundamental a la protección de datos personales los Derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del Derecho a ser informado de quién posee sus datos personales y con qué fin, y el Derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.»

---

no cercano la Carta de los Derechos Fundamentales de la Unión Europea adquiere relevancia máxima. E. Pedraz Penalva «La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva» en E. Pedraz Penalva (ed.) *Protección de datos y proceso penal,* Madrid: La Ley, 2010, págs. 24 y ss.

[22] PIÑAR MAÑAS, J.L. y CANALES GIL, A. Legislación de Protección de Datos, Madrid: Iustel, 2011, págs. 30 y ss.

De este Fundamento Jurídico se puede deducir el contenido esencial del derecho fundamental a la protección de datos que viene constituido por los principios y características que lo definen. Estos principios pueden quedar fijados en los siguientes: Consentimiento, información, finalidad, calidad de los datos, proporcionalidad y seguridad. Ahora bien para que estos principios puedan ser efectivos es necesario el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición de los que es sujeto activo el titular de los datos. Partimos de que el derecho fundamental a la protección de datos se fundamenta en el poder de disposición del titular sobre sus propios datos y que, como consecuencia del ejercicio de ese poder de disposición, existirán terceros que tratarán esos datos. Por tanto, si los datos sometidos a tratamiento son datos ajenos y se utilizan dentro del marco de respeto al poder de disposición de la persona es indudable que cuando se recojan esos datos haya que informar al interesado, debe existir un título que habilite su utilización, el titular debe consentir, el uso se debe hacer para las finalidades legítimas para las que fueron recabados, se debe respetar la proporcionalidad y mínima injerencia en el tratamiento, el uso debe ser leal y lícito y, todo ello se debe llevar a cabo, adoptando en el tratamiento las medidas de seguridad adecuadas[23].

Pues bien en relación con el ejercicio por el individuo, persona física titular de los datos, de este derecho fundamental a la protección de datos trataremos a continuación una cuestión puntual que se plantea en un entorno de informática ubicua: la captación de datos personales sin conocimiento de su titular.

III.2. La captación ubicua de datos personales

Como hemos expuesto en el planteamiento inicial los entornos de informática ubicua han multiplicado los lugares y métodos de captación de datos personales del individuo llegando incluso, en algunos

[23] La obligación de información al interesado queda recogida en los arts. 10 y 11 de la Directiva 95/46/CE, en el art. 5 de la LOPD y en los arts. 18 y 19 del Reglamento RD 1720/2007; el consentimiento del interesado, titular del dato, se regula en el art. 7 de la Directiva, art 8 de la Carta Europea de Derechos Fundamentales, en los arts. 6, 7 y 11 de la LOPD y en los arts. 12 a 17 del Reglamento. El principio de uso para la finalidad legítima para la que se recabó el dato en los arts. 6.1.a) de la Directiva, art. 4 de la LOPD y arts. 8 y 9 del Reglamento; por último el principio de seguridad se recoge en los arts. 16 y 17 de la Directiva; art. 9 de la LOPD y art. 79 y ss. del Reglamento. J.L. Piñar Mañas y A. Canales Gil, *Legislación de Protección de Datos, cit.*, pág. 35.

casos, a captar de manera inconsciente y, por tanto, inconsentida dichos datos de su titular.

Una nueva cuestión que se plantea es cómo ejercen los individuos su derecho fundamental a la protección de datos ante una nueva realidad en la que la proliferación de terminales que permiten la gestión de la identidad de los individuos son de uso habitual (móviles, ordenadores, tarjetas inteligentes) y permiten el tratamiento invisible de datos personales.

Es conocido por todos cómo muchos tratamientos de datos personales en Internet se llevan a cabo sin el conocimiento de la persona titular de los mismos, es decir, en un entorno invisible para ella. El Grupo de Trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, en su Recomendación 1/1999[24] ya destacó que los productos de *software* o *hardware* de Internet deberían permitir al usuario conocer tres aspectos fundamentales: 1.º qué datos del usuario se van a recoger; 2.º con qué fin se recogerán dichos datos y 3.º cómo acceder de forma fácil en un momento posterior a los datos recogidos.

Son tres aspectos básicos que responden a las exigencias del derecho fundamental a la protección de datos, apuntadas en la STC 292/2000, pero que para su efectivo cumplimiento requieren un cambio técnico sustancial en muchos navegadores actuales, enlaces en webs y *cookies*. Como veremos a continuación, los *cookies* pese a su aparente inofensivo nombre representan una amenaza real al derecho a la protección de datos de los individuos.

El grupo de trabajo del artículo 29 define los *cookies* como: «datos creados por un servidor web que pueden almacenarse en ficheros de texto que pueden colocarse en el disco duro del usuario de Internet, mientras una copia puede conservarse en el sitio web. Son una parte normal del tráfico HTTP, y pueden, por tanto, transportarse sin obstáculos con el tráfico IP. Un *cookie* puede contener un número único (GUI, identificador global único), que permite una mejor personalización que las direcciones IP dinámicas. Permite al sitio web guardar un rastro de las prácticas y preferencias del usuario. Los *cookies* contienen una serie de URL (direcciones) para las cuales son válidos. Cuando el navegador vuelve a encontrar estos URL, envía

[24] Working Party on the Protection of Individuals with regard to the Processing of Personal data. *Recommendation 1/99, on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.* 23 february 1999. 5093/98/EN/final WP 17.

los cookies específicos al servidor web. Los *cookies* pueden ser de naturaleza diferente: pueden ser permanentes o tener una duración limitada (los denominados cookies de sesión)»[25].

En este escenario de pluralidad de lugares donde los datos de un individuo pueden ser captados, en una «sociedad de riesgo ambiental», como la denomina la Profesora Llácer, no es solo la acomodación a la legalidad en el tratamiento del dato personal, como dato atribuible a una persona identificada o identificable, lo que ha de analizarse sino también el tratamiento del dato anónimo que genera un perfil no personal pero que puede provocar discriminación en el caso concreto, como en el caso expuesto de los *cookies*.

Siguiendo con este análisis y sin ánimo de plantear una visión opresiva, sino más bien lo más cercana posible a la realidad de la sociedad actual, podemos afirmar que vivimos en una sociedad de la identificación y de la incardinación de las personas en perfiles preestablecidos. En este sentido el Grupo de trabajo del artículo 29 en el Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE[26], hace referencia al suministro de datos, sea de forma consciente o inconsciente, por el usuario de Internet que permite crear perfiles de usuarios. En este caso nos estamos refiriendo a perfiles no personales pero que pueden provocar *ad hoc* una situación de discriminación. Aunque no nos encontremos en un entorno de tra-

[25] Grupo de trabajo del artículo 29 sobre Protección de Datos. *Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE,* Aprobado el 30 de mayo de 2002, (5035/01/ES/Final WP 56). Págs. 10-11. El mismo Grupo del artículo 29 en su *Recomendación 1/1999* en relación con los tres aspectos fundamentales apuntados, y para dar cumplimiento a los mismos, en lo referente con los cookies entiende que el usuario debe ser informado en el momento en que un cookie está intentando ser recibido en el equipo local, o almacenado o bien enviado por el navegador y se le debe dar al usuario la opción de aceptar o no su recepción. En todo caso hay que tener en cuenta que la cookie identifica el ordenador del usuario no al usuario mismo pero esta información anónima se trata con el fin de futuras identificaciones de ese ordenador en futuras visitas a la misma página web desde la que se envió la cookie pasando ya a un tratamiento decisional que sí afecta a un individuo. Cfr. *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.* 5093/98/EN/final WP 17. Pág. 3.

[26] Grupo de trabajo del artículo 29 sobre Protección de Datos. *Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE,* Aprobado el 30 de mayo de 2002, (5035/01/ES/Final WP 56). Págs. 10-11.

tamiento de información personal *stricto sensu* el tratamiento tiene fines decisionales sobre el individuo, aunque en principio se esté trabajando sobre información anónima. Volvemos así al concepto ya expuesto de *cookies* que, como práctica muy extendida de recogida de datos personales por medio de un fichero de texto, permite crear dichos perfiles no personales y posteriormente adscribir al individuo a uno de estos perfiles ya creado.

Es aquí en el tratamiento del dato anónimo donde algunos autores han planteado un nuevo problema denominado «*gap* informativo»[27], problema que afecta de modo directo al ejercicio del derecho fundamental a la protección de datos. Para Llácer Matacás la personal y voluntaria participación en la sociedad de la información sitúa al individuo, o puede situarlo en algunos casos, en un entorno de riesgo informacional en un doble sentido: por una parte al desconocer la captación de un dato personal de su titularidad desconoce su posterior tratamiento y, por otra parte, desconociendo esta captación y tratamiento no utiliza los medios jurídicamente a su alcance para su control, más arriba apuntados. Con ello podemos encontramos en una situación en la que el titular de los datos está a merced del poder ajeno, es decir, a merced del responsable de dicho tratamiento produciéndose así el «*gap* informativo citado que, en definitiva, alude a la fractura o desequilibrio en la base de la estructura de la sociedad de la información como organización social.

La simetría entre captación del dato y tratamiento debe ser perfecta para permitir al individuo el ejercicio de su derecho fundamental a la protección de datos. Si la vía de conexión, en el sentido de conocimiento, entre dato captado y tratamiento del dato está rota el ejercicio del derecho de control, de autodeterminación, se hace inviable y el efecto re-equilibrador de poderes se rompe produciendo una asimetría de poder en favor del responsable de ese tratamiento. Es decir, esta asimetría informativa, entre titular del dato y responsable del tratamiento, produce una asimetría de poder en favor del responsable. Al ser un tratamiento desconocido para el titular del dato éste no puede neutralizar jurídicamente, con el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, la asimetría de poder que dicho tratamiento produce.

Volvemos así al planteamiento expuesto más arriba por los Profesores Sánchez González y De Vega donde los derechos y la libertades, y en concreto el derecho a la protección de datos, han de

[27] LLÁCER MATACÁS, M.R. «La autodeterminación informativa en la sociedad de la vigilancia: *Ubiquitous Computing*», *cit*. Págs. 69 y ss.

concebirse ya no solo frente al poder del Estado sino también ante el conjunto de los poderes privados, calificables de auténticas coerciones fácticas. Se desarrolla así un juego de fuerzas entre desiguales donde el derecho fundamental ha de desempeñar un papel re-equilibrador y donde las asimetrías informativas que pueden implicar asimetrías de poder sean contrarrestadas por el derecho fundamental a la protección de datos al que cada vez cabe atribuir mayor relevancia en el ámbito del derecho privado.

III.3. La externalización de servicios TIC. Servicios *cloud*

En paralelo a la informática ubicua que hemos considerado, y precisamente porque la misma proporciona la infraestructura tecnológica necesaria, hoy se está desarrollando un modelo de prestación de servicios tecnológicos que permite, bajo demanda y a través de la Red, acceder a un conjunto de recursos *hardware* y *software* imprescindibles para empresas, profesionales o particulares desde cualquier punto geográfico del planeta, de forma fácil y con total transparencia para el usuario. En definitiva, el acceso a dichos servicios en la nube, *cloud* en referencia a Internet, plantea, entre otras cuestiones, una externalización de tratamientos de datos personales que antes se llevaba a cabo en local pero ahora se llevan a cabo en Internet.

Muchos de los servicios informáticos que se prestan en la *cloud* parten de la externalización o *outsourcing* de ese mismo servicio que antes era prestado en local, con los equipos, *software* y personal de la propia empresa, institución o profesional. Si se toma la decisión de externalizar, o contratar en *outsourcing,* algunas o todas de las actuaciones en relación con las tecnologías de la información y las comunicaciones es por dos razones fundamentales: por una parte, para centrarse en lo que realmente cada uno sabe hacer y aprovechar la especialización de otras compañías cuyo negocio son las TIC y, segundo, por motivos estrictamente económicos de ahorro de costes fijos y de estructura. Cabría añadir una tercera razón relacionada con el traslado del riesgo del cumplimiento de la normativa y, en concreto, de la normativa de protección de datos al proveedor que presta el servicio externalizado y, así mismo, el traslado de los riesgos de la seguridad de la información[28].

[28] SAIZ PEÑA, C.A.«La externalización de los Servicios TIC de una Organización. El caso práctico del outsourcing del Servicio de Atención a Usuarios. Aproximación a los aspectos de protección de datos, riesgos contractuales y análisis de riesgos de

La Comisión Jurídica del CGAE define el *Cloud Computing* como «un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios[29].

Las características de este modelo de prestación de servicios en la nube están expuestas con extrema claridad en el mismo Informe 3/2011 del CGAE y se concretan en cinco: autoservicio bajo demanda, múltiples formas de acceder a la red, compartición de recursos, elasticidad y servicio medido[30].

De las muchas posibles implicaciones jurídicas y técnicas que pueden derivarse de un modelo como el expuesto sólo nos detendremos en aquellas que se derivan del hecho de que los datos personales de los individuos, que obran legítimamente en poder de un responsable de fichero o de tratamiento[31], se transfieren a un sistema in-

seguridad de la información», Revista Española de Protección de Datos n.º 5, julio-diciembre 2008, pág. 276.

[29] Comisión Jurídica del Consejo General de la Abogacía Española, Informes 2011, Informe 3/2011 *Utilización del cloud computing por los despachos de abogados,* Valencia: Tirant lo Blanch, 2012, págs. 45 y ss.

[30] «1. Autoservicio bajo demanda. El usuario puede acceder a capacidades de computación «en la nube» de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios *Cloud*.

2. Múltiples formas de acceder a la red. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario, desde teléfonos móviles a ordenadores portátiles o *PDAs*.

3. Compartición de recursos. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque sí es posible que sean conscientes de su situación a determinado nivel, como el de CPD o el de país.

4. Elasticidad. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

5. Servicio medido. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, lo que posibilita el pago por el uso efectivo de los servicios.»

Comisión Jurídica del Consejo General de la Abogacía Española, *Informes 2011, cit.,* pág. 45.

[31] La LOPD lo define en su artículo 3.d) como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. No se debe entender que se puede denominar de una

formático, servidor, que puede estar ubicado en cualquier punto del planeta. El entorno tecnológico planteado en un modelo *cloud* hace que el ejercicio del derecho fundamental a la protección de datos lejos de diluirse haya de desarrollarse también en él.

IV. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN UN MODELO DE CLOUD O DE SERVICIOS TIC EXTERNALIZADOS

Como hemos expuesto en el punto anterior, los datos en el modelo de «*cloud computing* pasan a situarse en algún lugar indeterminado de la nube, de Internet, en un servidor cuya ubicación física *a priori* se desconoce.

La decisión de externalización de algunos procesos de información puede llevar consigo importantes consecuencias en el ámbito de la seguridad de la información, y cómo no, en el del cumplimiento de la normativa de protección de datos de carácter personal.

Considerando los aspectos jurídicos de esta externalización, en lo que se refiere a la protección de los datos personales, en todo modelo *cloud* han de diferenciarse claramente dos figuras: el responsable del fichero y el encargado del tratamiento. Quien pone en manos de su proveedor de servicios *Cloud* sus ficheros de carácter personal es el «responsable del fichero (art. 3 LOPD), y el proveedor de servicios *Cloud* es el «encargado del tratamiento del fichero (art. 3 LOPD), estando obligado, según el art. 12 LOPD, a seguir las instrucciones del responsable del fichero en el tratamiento de los datos.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[32], establece en su art. 12.2 que «*La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente*

u otra forma al responsable ya que hay muchos supuestos de hecho en los que cabe distinguir dos responsables: uno del fichero y otro del tratamiento. Sin embargo, la Directiva 95/46/CE en su artículo 2.d) habla solo de responsable del tratamiento como: «*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario*».

[32] BOE núm. 298, de 14 de diciembre de 1999.

tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas».

De aquí se derivan las siguientes consecuencias:

1.ª La propiedad de los datos que se van a albergar en la nube es de quien externaliza el tratamiento, y por tanto, el proveedor no puede disponer de ellos ni hacer uso de los mismos para ningún fin que no esté expresamente autorizado por aquel.

2.ª Debe existir un contrato de prestación de servicios entre el que externaliza el tratamiento de los datos, el responsable, y su proveedor de servicios *Cloud,* donde se recojan las previsiones necesarias para garantizar el adecuado cumplimiento de la normativa relativa a la protección de datos.

3.ª De acuerdo con lo dispuesto en el art. 12.4 LOPD el proveedor de servicios no puede dar a los datos un uso distinto al especificado por el responsable y en caso contrario el encargado del tratamiento pasaría a asumir la condición de responsable del fichero.

4.ª El encargado del tratamiento debe articular las medidas de seguridad necesarias para dotar a los datos de la protección adecuada a su nivel ya que conforme con el art. 7 LOPD hay datos que pertenecen a la categoría de datos especialmente protegidos (ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual,) para los que las medidas de seguridad son de nivel alto. Los art. 89 y siguientes del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (RLOPD)[33] desarrollan cuáles son las medidas exigibles al encargado del tratamiento para cada nivel de seguridad de los datos.

5.ª Los derechos de acceso, rectificación, cancelación y oposición se podrán ejercitar por el titular de los datos ante el responsable del fichero o ante el encargado del tratamiento pero en este segundo caso con las especialidades recogidas en el artículo 26 del RLOPD[34].

[33] BOE núm. 17, de 19 de enero de 2008.

[34] «*Artículo 26. Ejercicio de los derechos ante un encargado del tratamiento.–Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.*»

Las cinco consecuencias apuntadas tienen una validez general para modelos de servicios en la nube que implique tratamiento de datos personales, pero hay que tener en cuenta que cabe la posibilidad, nada improbable, de que los datos no se almacenen por el encargado en territorio español. Esto plantearía el problema de que la LOPD carece de fuerza de obligar fuera de España y nos situaría ante un supuesto de hecho en el que vienen en aplicación las disposiciones relativas a la transferencia internacional de datos. La Directiva 95/46/CE contempla en su artículo 25 la transferencia de datos personales a países terceros, señalando que la transferencia ha de limitarse a naciones en las que los datos cuenten con «un nivel de protección adecuado».

Por consiguiente, hay que distinguir dos posibilidades: el caso para el que en el país en el que se ubiquen los datos exista una legislación equiparable que garantice un adecuado nivel de protección, y el caso en que no.

Si el proveedor desarrolla el tratamiento dentro de la Unión Europea podemos considerar que nos encontramos en el primer escenario de nivel de protección adecuado donde el proveedor asumiendo expresamente el papel de encargado del tratamiento de los ficheros trasladados a la nube por el responsable asume, así mismo, todas las obligaciones propias de tal figura. Otro escenario es aquél en el que el proveedor almacena la información de carácter personal en sistemas ubicados físicamente fuera de la Unión Europea. En este caso cabría entender, en una interpretación garantista del problema, que debe firmarse un contrato entre el responsable y el proveedor de servicio *cloud* donde éste asuma las obligaciones que al encargado del tratamiento impone la legislación europea, con independencia del Derecho aplicable al lugar donde efectivamente se localizan los centros de proceso de datos.

En definitiva, el proveedor ha de garantizar que la información solo será accesible al responsable que contrata sus servicios, y a quienes éste determine y debe articular los mecanismos necesarios para que los titulares de los datos puedan acceder a sus datos y no a los de otros. Para ello las medidas técnicas y organizativas son imprescindibles. Así mismo, el proveedor ha de disponer de los mecanismos de recuperación ante desastres, continuidad en el servicio y copia de seguridad necesarios para garantizar la integridad y conservación de la información.

Todo lo expuesto atiende a la finalidad de diseñar un ámbito de seguridad jurídica donde en el caso de incumplimiento del provee-

dor de servicios *Cloud* de las obligaciones anteriormente recogidas, tanto el responsable del fichero como los propios titulares de los datos puedan ver protegidos sus respectivos derechos. La última cuestión que cabría plantear es la posibilidad de atribuir responsabilidad solidaria entre responsable y encargado en caso de vulneración de los derechos de los titulares de los datos.

V. CONCLUSIONES

El consentimiento del titular de los datos para su tratamiento es la piedra angular del derecho fundamental a la protección de datos. Hemos apuntado en estas páginas amenazas cotidianas que nos proporciona la sociedad de la información en la que todos estamos inmersos. Una de esas amenazas es, sin duda, la ausencia de consentimiento en el tratamiento de nuestros datos por desconocimiento del mismo.

Podemos afirmar que nos encontramos ante un sistema de organización social de riesgo colectivo para la protección de nuestros datos personales. Bien sea porque ignoramos la captación de datos dejados en el uso de los medios de acceso a Internet, bien sea la adscripción a perfiles personales con fines decisionales, o bien porque nuestros datos se encuentran en un lugar indeterminado dentro de la gran nube que constituye la Red, lo cierto es que se cuestiona la eficacia del derecho fundamental a la protección de datos como única arma defensiva en poder del individuo. Son por ello el ejercicio de los recursos jurídicos y técnicos adecuados los que podrán devolver al titular de los datos el control sobre ellos y, en definitiva, sobre el libre desarrollo de su personalidad.

El derecho a la protección de datos, que desde distintos supuestos de hecho hemos planteado en estas páginas, necesita un doble nivel de defensa: jurídico y técnico. Con la prestación del consentimiento y ejercicio de los derechos de acceso, rectificación, cancelación y oposición la tutela jurídica se llena pero debe existir un nivel de defensa preventivo técnico en el que el derecho a la protección de datos encuentre pleno amparo.