APROXIMACIÓN A LA REGULACIÓN DEL CONSENTIMIENTO EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Carlos Trujillo Cabrera*
Universidad de La Laguna

Resumen

El 25 de mayo de 2018 entró en vigor el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, que modifica en gran medida el régimen que hasta ahora se venía aplicando por la Directiva 95/46/CE y la Ley Orgánica de Protección de Datos que la transponía. El presente trabajo realiza una aproximación inicial al tratamiento que del consentimiento se ha venido realizando en la referida normativa en materia de protección de datos, y en qué medida ese tratamiento va a verse modificado como consecuencia de la aprobación del Reglamento, con la finalidad de determinar si dichas modificaciones constituyen o no una mejora a la protección de los titulares de los datos sometidos a tratamiento.

Palabras clave: tratamiento de datos, consentimiento, reglamento general de protección de datos.

THE CONSENT TO DATA PROCESSING IN THE NEW EUROPEAN GENERAL DATA PROTECTION REGULATION

Abstract

On 25th May 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which greatly modifies the regime that has so far been applied by Directive 95/46/EC and the *Ley Orgánica de Protección de Datos* that transposed it, entered into force. This paper provides an initial approach to the processing of consent in the aforementioned legislation on data protection, and the extent to which such processing will be modified as a result of the adoption of the Regulation, in order to determine whether or not such modifications constitute an improvement in the protection of the data subjects subject to processing.

Keywords: personal data processing, consent, european law.

DOI: http://doi.org/10.25145/j.anfade.2017.34.004
Anales de la Facultad de Derecho, 34; septiembre 2017, pp. 67-75; ISSN: e-2530-8319

INTRODUCCIÓN

Desde principios de los años setenta, los avances experimentados a la hora de recoger y tratar datos han puesto de manifiesto la necesidad de establecer mecanismos jurídicos que permitan proteger a las personas de los riesgos que se derivan de un posible tratamiento indebido de sus datos personales. Desde esta perspectiva, la privacidad de los datos personales ha estado estrechamente relacionada con la denominada autodeterminación informativa[1], argumentando que las personas deberían poder determinar de forma independiente qué tipo de información sobre sí mismas se puede recopilar y tratar, así como las circunstancias y condiciones de dicha recopilación y tratamiento.

Con esta finalidad, las normas en materia de protección de datos han tenido precisamente como objetivo el garantizar la autodeterminación de las personas, fundamentalmente a través de la posibilidad de tomar una decisión con conocimiento de causa y de optar por aceptar o rechazar las condiciones de recogida y tratamiento de datos, expresando libremente –o denegando– su consentimiento con conocimiento de causa.

El presente trabajo pretende únicamente realizar una aproximación inicial al tratamiento que de dicho consentimiento se ha venido realizando en la normativa en materia de protección de datos (tanto en la europea como en la estatal), y en qué medida ese tratamiento va a verse modificado como consecuencia de la aprobación del Reglamento General de Protección de Datos, cuyos efectos comenzarán a desplegarse el próximo 25 de mayo de 2018, con la finalidad de determinar si dichas modificaciones constituyen o no, en realidad, una mejora a la protección de los titulares de los datos sometidos a tratamiento, como el Reglamento parece afirmar.

ANALES DE LA FACULTAD DE DERECHO, 34; 2017, PP. 67-78

EL CONSENTIMIENTO COMO CONTENIDO ESENCIAL DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El derecho a la protección de datos personales encuentra su primer antecedente en el artículo 12 de la Declaración Universal de los Derechos del Hombre, en el que se afirmaba que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o

---

* Prof. ayudante doctor (acreditado contratado doctor).

[1] Fórmula tomada de la Sentencia del Tribunal Constitucional Federal de Alemania de 15 de diciembre de 1983 sobre la Ley del Censo, y que hace referencia al control que ofrece a las personas sobre el uso que puedan hacer terceros de información sobre ellas mismas. A pesar de no estar recogida como tal en el Derecho positivo, ha tenido gran aceptación en la doctrina. *Vid*., en este sentido, P.L. Murillo de la Cueva, «La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad», en P.L. Murillo de la Cueva y J.L. Piñar Mañas, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 11 y ss.

a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques», y fue posteriormente recogido en numerosos cuerpos normativos, como el Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales o el Pacto de los Derechos Civiles y Políticos, o el Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en el que solo se consideraba lícita la utilización de estos datos por un tercero cuando los mismos se hubieran obtenido con el consentimiento inequívoco de los afectados, debidamente informados, o con autorización legal explícita[2].

En el caso concreto de España, la primera referencia se encuentra en el artículo 18.4 de la Constitución española, que dispone 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», y cuyo mandato dio lugar a la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

Sin embargo, en el año 1995 se aprobó el que sería a partir de entonces el texto europeo de referencia en materia de protección de datos personales, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, 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. Esta Directiva fue transpuesta en España de la mano de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de desarrollo.

Ambas normas tomaron como base el art. 18.4 CE, tal y como refrendó el Tribunal Constitucional en su Sentencia 292/2000 [RTC 2000, 292], en la que afirmaba que en varias decisiones anteriores el Tribunal ya había declarado que el art. 18.4 CE contenía, en los términos de su Sentencia 254/1993 [RTC 1993, 254], un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, era en sí mismo «un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática"», lo que se ha dado en llamar «libertad informática» (F. 6, reiterado luego en numerosas sentencias posteriores [RTC 1994, 143; RTC 1998, 11; RTC 1998, 94; RTC 1999, 202].

A partir de esta afirmación, establecía el Tribunal Constitucional que la garantía de la vida privada de la persona y de su reputación posee una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. De esta manera, esa llamada «libertad informática» constituye un derecho a controlar el uso de los mismos datos insertos en un programa informático («habeas data») y comprende, entre otros aspectos, la oposición del ciudadano a que

[2] P.L. Murillo de la Cueva, *op. cit.*, p. 26.

determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

De esta manera, el contenido esencial[3] 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.

EL CONSENTIMIENTO EN LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, Y EN SUS NORMAS DE DESARROLLO

La propia Directiva 95/46/CE, de la que trae causa la vigente LOPD, dispone que todo tratamiento de datos personales exige una base jurídica que lo legitime. Tales bases jurídicas están tasadas en su artículo 7, que solo considera como legítimas la existencia de consentimiento inequívoco del afectado o bien que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte, el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, la protección del interés vital del interesado, el cumplimiento de una misión de interés público, o la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

De lo indicado hasta ahora resulta evidente que el principio del consentimiento constituye uno de los pilares esenciales del derecho fundamental a la protección de datos[4], de tal manera que el mismo solo podrá ser obviado en los casos en que una norma con rango de Ley así lo justifique[5]. Tal es el sentido que se desprende del artículo 6 LOPD cuando afirma que «el tratamiento de datos de

[3] J. Plaza Penadés, «El nuevo modelo de protección de datos personales europeo y el modo de obtener un consentimiento lícito», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 44, Navarra, 2017, p. 26.

[4] J. Morales Barceló, «Big Data y protección de datos: especial referencia al consentimiento del afectado», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 44, Navarra, 2017, p. 151.

[5] J. Álvarez Hernando, *Practicum Protección de Datos 2018*, Aranzadi, Navarra, 2017, p. 94.

carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa».

En este sentido, tanto el artículo 2 de la Directiva 95/46/CE como los artículos 3.h) LOPD y 5.1.d) de su Reglamento definen el consentimiento como «toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen».

Por tanto, para que el consentimiento pueda constituir una base jurídica legítima para el tratamiento de datos personales, es necesario que el mismo cumpla con una serie de requisitos. En primer lugar, el consentimiento debe ser libre, sin que exista, por tanto, ningún tipo de coacción, coerción o imposición. Además, el consentimiento debe ser inequívoco[6], y, por tanto, sin que haya dudas acerca de que el mismo se ha producido[7]. Nótese, sin embargo, que la necesidad de que sea inequívoco no afecta a la forma en que pueda manifestarse, no siendo necesario que el consentimiento se preste de forma expresa[8] o de forma escrita[9], salvo que nos encontremos ante el tratamiento de datos personales que revelen la ideología, afiliación sindical, religión y creencias[10], en cuyo caso el artículo 7.2 LOPD exige que el consentimiento sea expreso y por escrito[11], y siempre que, previamente, se informe al titular de los datos de que no está obligado a proporcionarlos (artículo 7.1 LOPD).

Por último, es necesario que el consentimiento sea específico, esto es, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima; y que sea informado, de manera que el afectado debe conocer y ser plenamente consciente, con anterioridad al tratamiento, de su existencia y de las finalidades para las que se produce.

De los anteriores requisitos que deben configurar el consentimiento válidamente emitido se deriva la posibilidad de que el consentimiento, salvo en el caso de datos sensibles, pueda ser tácito, entendido como tal aquel consentimiento que se deriva de una falta de actividad por parte de un interesado que es consciente y conoce que se está produciendo un tratamiento con sus datos personales. No obstante lo

---

[6] J.M. Fernández López, «Artículo 6. Consentimiento del afectado», Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, 2010, p. 454 y ss.

[7] Sentencia de la Audiencia Nacional, Sección Primera, de 13 de abril de 2005 (JUR 2006, 238672), que destaca cómo el requisito de inequívoco, derivado de la Directiva 95/46/CE, constituye una novedad respecto de la anterior regulación contenida en la LORTAD.

[8] Regulado con mayor detalle en el artículo 14 del Reglamento de la LOPD. *Vid*. J. Zabía de la Mata, «Artículo 14. Forma de recabar el consentimiento», Protección de Datos. Comentarios al Reglamento, Lex Nova, 2008, p. 193 y ss. Igualmente, dispone el Informe Jurídico 000/2000, de la Agencia Española de Protección de Datos, que «de lo que se ha indicado se desprende que de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente...».

[9] De acuerdo con el Informe Jurídico 0081/2009, de la Agencia Española de Protección de Datos, pág. 3, «para que pueda hablarse de consentimiento inequívoco se exige la realización de una acción u omisión que implique la existencia del consentimiento».

[10] P.L. Murillo de la Cueva, *op. cit.*, p. 51.

[11] P.L. Murillo de la Cueva, *op. cit.*, p. 50.

anterior, dicho consentimiento tácito debía ser tratado «con gran delicadeza» cuando estaban en juego «derechos constitucionales básicos»[12].

EL CONSENTIMIENTO EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LOS POSIBLES PROBLEMAS QUE PUEDEN DERIVARSE

El *Diario Oficial de la Unión Europea* publicó el 4 de mayo de 2016 el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE; más conocido por el nombre «Reglamento General de Protección de Datos». Aunque de acuerdo con su artículo 99, el RGPD entró en vigor a los veinte días de su publicación en el *DOUE*, se establecía en el apartado segundo de dicho precepto que será aplicable a partir del 25 de mayo de 2018.

El RGPD regula en su artículo 4.11 el concepto de consentimiento del interesado en los siguientes términos: «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». De esta manera, resulta evidente que el consentimiento solo puede expresarse de dos formas: bien mediante una declaración, o bien mediante una acción, en ambos casos debiendo ser clara y afirmativa. Por ello, el consentimiento tácito ya no sería posible[13]. Por su parte, el considerando (32) del RGPD refuerza esta afirmación al aclarar determinadas situaciones que no pueden tener la consideración de consentimiento: el silencio, las casillas previamente seleccionadas o la inacción[14]. Por tanto, el RGPD exige que el consentimiento sea siempre expreso y que el mismo abarque a todas las finalidades que vaya a tener el tratamiento de los datos.

Tal y como indica el RGPD en sus primeros considerandos, fundamentalmente los (6), (7), (8) y (9), la finalidad del mismo no es otra que reforzar la protección jurídica de las personas que se mueven en un mundo cada vez más tecnológico y globalizado, en el que los datos personales son utilizados por empresas privadas y autoridades públicas a una escala sin precedentes, y en el que la inseguridad jurídica es cada vez mayor en relación con la protección que se dispensa a las personas físicas, especialmente en sus actividades en línea; lo que se pretende conseguir, entre otras medidas, reforzando el control que el titular de los datos tiene sobre el tratamiento que de los mismos se haga, de tal manera que será necesario su consentimiento expreso

[12] Sentencia de la Audiencia Nacional, Sección Primera, de 7 de julio de 2000 (RJCA 2001, 73).

[13] B. Adsuara Varela, «El consentimiento», en J.L. Piñar Mañas (dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Zaragoza, 2016, p. 152.

[14] J. Plaza Penadés, *op. cit.*, p. 37.

para poder llevar a cabo un tratamiento de datos que no se encuentre autorizado por una norma con rango legal.

Este énfasis en la autodeterminación informativa en materia de protección de datos puede parecer, inicialmente, el camino correcto[15], pero parte, a mi juicio, de una idea errónea acerca de cómo actúan los titulares de datos, especialmente en sus relaciones y actividades en línea, donde suelen prestar su consentimiento siempre que se les pide, sin entender a qué y por qué están consintiendo realmente. Consideran en este sentido algunos autores[16] que lo anterior es muestra de una desconexión entre la teoría jurídica, que presupone un titular de los datos racional e informado que toma decisiones conscientes, y la realidad práctica, en la que los titulares de los datos simplemente otorgan su consentimiento sin entender a qué están consintiendo, lo que implica riesgos tanto para los titulares (que pueden consentir involuntariamente a tratamientos no deseados de datos) como para los responsables del tratamiento (que no pueden confiar plenamente en el consentimiento que obtienen). De esta manera, se disminuye el control que los titulares tienen sobre sus datos personales, se crea una falsa sensación de confianza y, en última instancia, se aumentan los riesgos para la privacidad[17].

Como bien se ha señalado[18], cuando se solicita al titular su consentimiento para el tratamiento de datos se le está en realidad advirtiendo que puede tener lugar una transformación potencialmente dañina o legalmente significativa que requiere la atención plena del individuo. Pero en la práctica, lo cierto es que los usuarios rara vez leen los avisos de privacidad, o no los comprenden totalmente, y sin embargo consienten el tratamiento de los datos personales.

Precisamente por ello, la regulación del consentimiento que pretende llevar a cabo el RGPD puede producir, fundamentalmente, dos efectos[19]:

1. Una sobrecarga de consentimientos, pues siempre tendrá que ser expreso, lo que implicará una disminución del efecto psicológico que su prestación lleva aparejada, de suerte que se reducirán los efectos del consentimiento como mecanismo de protección contra la divulgación no autorizada de datos.
2. Una sobrecarga de información, pues dada la gran complejidad del tratamiento de datos y los requisitos legales en materia de transparencia y notificación, los avisos de privacidad suelen ser textos largos, difíciles y de alto contenido técnico-jurídico, que, buscando evitar o reducir al mínimo la responsabilidad

[15] M.A. Davara Rodríguez, «Reglamento Europeo sobre protección de datos», *Actualidad Administrativa*, núm. 7, 2016, p. 3.

[16] B.W. Schermer, B. Custers y S. van der Hof, «The crisis of consent: how stronger legal protection may lead to weaker consent in data protection», *Ethics and Information Technology*, volumen 16, número 2, Berlin, 2014, p. 171.

[17] B.W. Schermer, B. Custers y S. van der Hof, *op. cit.*, p. 172.

[18] B.W. Schermer, B. Custers y S. van der Hof, *op. cit.*, *loc. cit*.

[19] B.W. Schermer, B. Custers y S. van der Hof, *op. cit.*, p. 176 y ss.

del responsable del tratamiento de los datos, se hacen tremendamente difíciles de entender por la generalidad de las personas a las que van dirigidos.

Lo anterior socava la noción básica de consentimiento, pues lo cierto es que el consentimiento no es plenamente informado si la persona que lo presta es incapaz de comprender las consecuencias que van aparejadas. En este sentido se manifiesta la ya citada STC 292/2000, al afirmar (FJ 6.º) que «el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos [...]. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin». A ello debe añadirse que, al menos en las actividades en línea, lo normal es que la solicitud de consentimiento se realice mientras el titular de los datos está inmerso en un proceso de toma de decisiones completamente diferente[20], como la reserva de las vacaciones, de manera que su no otorgamiento implicaría la privación de las mismas, especialmente si se tiene en cuenta que la mayoría de los servicios en línea utilizan los datos personales como pago por la prestación de un servicio que, en apariencia, resulta gratuito (especialmente notorio en las redes sociales, como Facebook o Instagram). En un contexto como este, en el que el titular de los derechos no tiene más opciones que otorgar el consentimiento, y disfrutar del servicio que desea, o no otorgarlo, y no poder por tanto acceder a ese servicio, resulta evidente que la idea de libertad en la prestación del consentimiento que exigen tanto la Directiva 95/46/CE como el RGPD se ve profundamente mermada, especialmente si, como establece el apartado 4 del artículo 7 del Reglamento, «al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato».

De esta manera, la sobrecarga de consentimiento y la sobrecarga de información conllevan una desensibilización del consentimiento, por cuanto los titulares no toman decisiones activas e informadas cuando se les pide el consentimiento, sino que se limitan a darlo sin sopesar sus posibles consecuencias[21].

[20] B.W. Schermer, B. Custers y S. van der Hof, *op. cit.*, p. 177.

[21] «The N&C [Note and Consent] mechanism is grounded on the assumption that the expression of consent by ticking a case signifies user knowledge and conscious acceptance of the contractual clauses of every service she utilizes. Such assumption seems more than questionable. Indeed, studies have demonstrated that individuals should spend 8 h a day for 76 days every year to read the ToS and PPs of the websites they visited on average». L. Belli, M. Schwartz y L. Louzada, «Selling your soul while negotiating the conditions: from notice and consent to data control by design», *Health and Technology*, volumen 7, número 4, Berlín, 2017, p. 456.

CONCLUSIONES

Parece evidente que en la actualidad, con la presencia del *big data*, las redes sociales y el denominado internet de las cosas, la necesidad de recabar un consentimiento individualizado del titular de los datos para cada procesamiento de los mismos que se pretenda llevar a cabo resulta complicado[22]. Siguiendo esta línea de pensamiento, no resulta aconsejable hacer descansar el grueso de la protección que se pretenda dispensar al titular en el consentimiento individual[23].

Frente a ello, se han postulado diversas hipótesis respecto a la mejor manera de acompañar este principio general del tratamiento basado en el consentimiento, bien sea pronunciándose a favor de una vuelta al consentimiento presunto[24], bien lo sea a favor de utilizar mecanismos adicionales de tutela que minimicen el número de datos personales tratados y aseguren que, por defecto, solo se tratarán los datos personales imprescindibles y necesarios para cada objetivo o finalidad específica del tratamiento[25]: son los llamados mecanismos de privacidad desde el diseño («Privacy by Design» o PbD en inglés).

A esta última hipótesis obedece precisamente el artículo 25 del Reglamento General de Protección de Datos, a cuyo tenor el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la pseudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados. De esta manera, se busca que solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento, afectando así a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad; y garantizando, en

[22] P. de Hert y V. Papakonstantinou, «The New General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law and Security Review*, núm. 32, 2016, p. 187, consideran que la idea es «absurda».

[23] S. Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg y M. Waidner, «Online Privacy: Towards Informational Self-Determination on the Internet», *Manifesto fromDagsthul Perspectives Workshop* 11061, 2011, p. 1 y ss.

[24] Para B.W. Schermer, B. Custers y S. van der Hof, *op. cit.*, p. 172, un beneficio añadido de este modelo de consentimiento es que reintroduce una medida de riesgo en el sistema de protección de datos, de manera que a partir del momento en que los interesados ya no puedan basarse en solicitudes de consentimiento expreso para advertirles siempre, es posible que se vean incentivados a prestar más atención a sus interacciones (especialmente las que se realicen *online*) y al papel de los datos personales en estas interacciones. Por ello, cuando los interesados se enfrenten a solicitudes de consentimiento expreso, el efecto de advertencia será mayor, pues serán conscientes de que la misma se produce por cuanto los datos solicitados o el uso que se les va a dar reviste una especial trascendencia.

[25] R.M. García Pérez, «La protección de datos de carácter personal del consumidor en el Mercado único digital», *Revista de Derecho Mercantil*, núm. 301, 2016, p. 11.

particular, que por defecto los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

El problema, sin embargo, radica en que la implementación de estas medidas por parte del responsable se supedita al principio de proporcionalidad que se vincula, por una parte, a la tecnología disponible (las «Privacy-Enhancing Technologies» o PETs[26]) y, por otra parte, a los costes de implantación, por lo que su efectividad parece hacerse depender de la capacidad económica del responsable y de su coste en relación con la cuenta de resultados de la empresa o entidad[27].

Será necesario, por tanto, esperar a que el citado Reglamento empiece a ser aplicado para poder determinar si las medidas implantadas por el mismo son suficientes y adecuadas para la finalidad pretendida por el legislador europeo o si, por el contrario, es necesario proceder a una revisión de las mismas.

Recibido: marzo de 2018, aceptado: abril de 2018

[26] L. Belli, M. Schwartz y L. Louzada, *op. cit*., p. 457, si bien consideran (*op. cit*., p. 459 y ss.) que los mecanismos de PbD no son suficientes por sí solos, y necesitan del complemento que otorgan los mecanismos de *Data Control by Design* (DCD), que son aquellos que se sustentan sobre la base de favorecer la proactividad del individuo, otorgándole las herramientas técnicas necesarias para evitar, *ab initio*, la recolección y el tratamiento de datos.

[27] J. Villarino Marzo, «La privacidad desde el diseño en la Propuesta de Reglamento Europeo de Protección de Datos», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 32, 2013, p. 45 y ss. En el mismo sentido, R.M. García Pérez, *op. cit*., loc. cit.