Foro, Nueva época, vol. 23, núm. 2 (2020): 149-182 ISSN: 1698-5583
https://dx.doi.org/10.5209/foro.77681

EL CONSENTIMIENTO EN LA ACTUAL NORMATIVA DE PROTECCIÓN DE DATOS: NUEVO PANORAMA JURÍDICO Y NUEVOS REQUISITOS

Isabel-Cecilia DEL CASTILLO VÁZQUEZ
Directora de la Inspección de Servicios
Delegada de Protección de Datos
Universidad Complutense de Madrid
icecilia@ucm.es

RESUMEN

Se analiza el sentido de los arts. 7 del Reglamento General de Protección de Datos (RGPD) y 6 de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDyGDD), en relación con los perfiles que debe presentar el consentimiento como fundamento jurídico específico para el tratamiento de los datos de tipo personal.

Palabras clave: consentimiento, protección de datos, afectado, datos personales, Derecho de la Unión Europea, Derecho español, Derecho nacional, transposición.

ABSTRACT

We hereby study the meaning of article 7 of General Data Protection Regulation (RGPD, in Spain) and article 6 of the Organic Act on the Protection of Data and Guarantee of Digital Rights (LOPDyGDD, in Spain), regarding the profiles entitled to the specifically legally binding consent to deal with personal data.

Keywords: Consent, Data Protection, Victim, Personal Data, EU Law, Spanish Law, Domestic Acts, Transposition.

ZUSAMMENFASSUNG

Es wird die Bedeutung von Artikel 7 der Allgemeinen Datenschutzverordnung (DSGVO) und Artikel 6 des Organgesetzes zum Datenschutz und zur Gewährleistung digitaler Rechte (LOPDyGDD) in Bezug auf die Profile, die der Einwilligung als spezifischer Rechtsgrundlage für die Verarbeitung personenbezogener Daten bedürfen, untersucht.

Schlüsselwörter: Einwilligung, Datenschutz, betroffene Person, personenbezogene Daten, Recht der Europäischen Union, spanisches Recht, nationales Recht, Umsetzung.

I. INTRODUCCIÓN

Caracterizado como un derecho de cuarta generación, a lo largo del siglo XX el derecho relativo a la protección de datos de carácter personal fue dejando clara su naturaleza inherente a la personalidad, hasta ser reconocido como derecho humano a través de los distintos instrumentos jurídicos internacionales.

A día de hoy, nadie discute que se trata de un derecho fundamental autónomo[1], vinculado a la dignidad y al libre desarrollo de la personalidad del ser humano que, a través del control de la información personal, se traduce en la reserva del espacio limitado que el individuo elige para quedar resguardado de las invasiones de terceros, ya procedan de sujetos privados o de la autoridad pública, y que dogmáticamente ha recibido el nombre de derecho a la autodeterminación informativa[2].

---

[1] *Vid.* arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Sobre este tema puede consultarse el extenso estudio realizado por I.-C. DEL CASTILLO VÁZQUEZ, *Protección de datos: cuestiones constitucionales y administrativas*, Cizur Menor, Aranzadi, 2007, principalmente pp. 238 y ss.

[2] El reconocimiento del derecho relativo a la protección de datos de carácter personal tiene como punto de partida la Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional de la República Federal Alemana sobre la Ley del Censo y el Derecho a la Personalidad y Dignidad Humana (ref. 1 BvR 209/83). A partir de esta sentencia, distintas voces se alzaron en la defensa de un criterio que va más allá de la intimidad del sujeto, pues lo que está en juego excede del perímetro de sus contornos para adentrarse en un núcleo más amplio y no ajeno a la privacidad del individuo.

La citada sentencia alemana examinó una demanda contra la Ley del Censo de Población de 1983 frente a la que se invocaba la lesión de los derechos protegidos en los arts. 1, 2, 5 y 19 de la Ley Fundamental de Bonn: *a)* derecho al libre desenvolvimiento de la personalidad y a la dignidad humana; *b)* libertad de expresión; *c)* garantías procesales, al estimar que dichos preceptos no satisfacían suficientemente los requisitos de constitucionalidad en cuanto a la recogida de datos y, sobre todo, en sus disposiciones sobre la utilización de los mismos. El Tribunal reconoció el derecho a la protección de datos de carácter personal bajo la denominación de «autodeterminación informativa» *(informationelle Selbstbestimmungsrecht),* por el cual el sujeto ostenta potestades e injerencia en el manejo que entidades públicas y privadas hagan sobre los datos personales que le conciernen. La sentencia definió los contornos del derecho, entendiendo que sus limitaciones han de quedar circunscritas a los

El contenido esencial del derecho a la autodeterminación informativa, enraizado en su génesis en el rechazo a cualquier intromisión en la vida privada del sujeto[3], otorga a su titular una posición jurídica de contenido positivo que se conforma sobre un haz de facultades destinadas a controlar el uso de su información personal tanto en el momento inicial de la recogida de datos como en fases posteriores del tratamiento. He aquí la delimitación conceptual del contenido esencial del derecho tratado. Definición a la que se alcanza bajo la determinación abstracta y genérica del mismo, y que, al compás de las pautas dictadas por De Otto, no indica ni las concretas facultades que comprende ni el concreto estatus jurídico del titular de la potestad de que se trata[4].

A partir de este punto, y entendiendo la individualidad de cada sujeto como la diferencia intrínseca de cada ser humano que lo hace único en su especie, la construcción legal del derecho se ha materializado en una tutela fundada en la libre decisión sobre qué datos propios desea su titular poner a disposición de terceros y qué utilización de los mismos autoriza[5]. Igualmente, y en el juego de graduaciones en la protección de las conductas y dentro de los contenidos adicionales, el derecho comportará la facultad de saber qué información personal obra en los múltiples

---

estrictos márgenes de un interés general superior y necesitan un fundamento legal basado en la Constitución. Además, decía el Tribunal, el legislador debe observar para su regulación el principio de la proporcionalidad y tiene que adoptar precauciones de índole organizativa y de Derecho procesal susceptibles de contrarrestar el peligro de vulneración del derecho a la salvaguardia de la personalidad.

Para un examen más detallado puede consultarse A. Podlech, «Art. 2, Abs. 1», en *Kommentar zum Grungesetz für die Bundesrepublik Deustchland (Rheine Alternativkommentare),* Neuwied-Darmstadt, Luchterhand, 1984, pp. 41 y ss., citado por A.-E. Pérez Luño, «Los derechos humanos en la sociedad tecnológica», *Cuadernos y Debates,* núm. 21 (1989), pp. 156, nota del autor 20.

[3] «Es cierto que toda persona tiene derecho a reservarse sus sentimientos si así lo desea. Tiene, ciertamente, derecho a juzgar si quiere hacerlos públicos o manifestarlos únicamente ante sus amigos». *Vid.* J. Yates en *Millar v. Taylor,* 4 Burr., 2303, 2379 (1769), citado por S. Warren y L. Brandeis, en B. Pendás y P. Baselga, *El derecho a la intimidad,* 1.ª ed., Madrid, Civitas, 1995, p. 31, nota al pie 16, publicado originalmente en 1890 bajo el título «The Rigth to Privacy», *Harvard Law Review,* vol. IV, núm. 5 (1890).

[4] L. Martín-Retortillo Baquer e I. de Otto y Pardo, *Derechos fundamentales y Constitución,* Madrid, Civitas, 1988, p. 159.

[5] Sobre todas estas cuestiones interesa destacar el artículo de R. García Mahamut, «El derecho fundamental a la protección de datos: el Reglamento (UE) 2016/679 como elemento definidor del contenido esencial del art. 18.4 de la Constitución», disponible en *https://dialnet.unirioja.es/descarga/articulo/6762711.pdf* (consultado el 31 de julio de 2021); trabajo desarrollado por la autora en el marco del proyecto de investigación sobre «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado», Ministerio de Economía y Competitividad (DER 2015-63635-R), del que es IP.

bancos de datos existentes. Implicará, asimismo, que el interesado pueda controlar el uso y transmisión que se va a hacer de los datos que obran en poder de un tercero, preservándolos de los demás cuando así lo decida, salvo que, más allá de su consentimiento, exista una base jurídica que legitime ese tratamiento. Lo que en sus aledaños enlazará con el conocimiento de la finalidad para la que se recaban, se almacenan, se comunican o, en general, se tratan los datos, de acuerdo con los principios relativos al tratamiento. Es decir, licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad. Todo ello bajo el principio de responsabilidad proactiva que impone el art. 5 del Reglamento (UE) núm. 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 (en adelante, RGPD), y por el que se deroga la Directiva 95/46/CE.

Reconocido como un derecho propio de sociedades avanzadas, el RGPD refuerza las garantías de este derecho al reedificarlo sobre la «privacidad desde el diseño y por defecto» *(«privacy by designe and by default»)* (art. 25)*,* que en la vida real supone un cambio de paradigma con la erradicación del consentimiento presunto, del consentimiento «universal» otorgado con un solo clic o de una vez para multitud de tratamientos y de los farragosos términos jurídicos y largos textos impregnados de condiciones abusivas[6] e ininteligibles para el común de los mortales. El *«privacy by design and by default»* viene, en suma, a entregar al individuo el control efectivo —que siempre debió estar en su poder— sobre sus datos personales[7].

---

[6] *Vid.* Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (*DO,* núm. L 95, de 21 de abril de 1993, p. 29), citada por el RGPD en su considerando 42.

[7] Considerando 6 RGPD: «La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales».

Considerando 7: «Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el

Los considerandos del Reglamento aportan valiosos elementos interpretativos que ayudan a perfilar con precisión el concepto de consentimiento que vierte el RGPD. Así, el considerando 40 RGPD nos aclara que:

> «Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato».

En este contexto, el consentimiento no solo se mantiene, sino que se refuerza como factor medular en el tratamiento de los datos de carácter personal. Bien es cierto que a día de hoy es solo uno de los seis fundamentos jurídicos del tratamiento que reconoce el RGPD; ni más ni menos, ni menos ni más.

En su transposición de la Directiva 95/46/CE, la Ley Orgánica 15/1999 otorgaba al consentimiento el valor de causa general e, incluso, de única causa legítima que operaba para el tratamiento de los datos[8], sin perjuicio de las obligaciones legales y con las salvedades señaladas en el apartado 2.º del art. 6 de dicha Ley[9]. En la actualidad, el consentimiento es un funda-

---

mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas».

Sobre este particular, *vid.* R. M. Miralles López, «Protección de datos desde el diseño y por defecto (comentario al art. 25 RGPD)», en A. Troncoso Reigada (dir.) y J. J. González Rivas (pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos,* vol. I, 1.ª ed., Pamplona, Civitas, 2021, pp. 1813-1818.

[8] Si bien en el Dictamen 15/2011, el GT29 aclaraba que el consentimiento es uno, pero no el único, fundamento de legalidad del tratamiento de datos personales. *Vid.* Dictamen 15/2011, de 13 de julio (WP 187), *On the definition of consent: «In sum, the legislative history, particularly in the EU, shows that consent has played an important role in conceptions of data protection and privacy. At the same time, it shows that consent has not been deemed as the only legal ground for legitimising data processing operations».*

[9] En este contexto, afirmaba en 2015 la autora Arenas Ramiro que: «El consentimiento es la llave de todo tratamiento de datos personales. Salvo excepciones legalmente previstas, el consentimiento da acceso al tratamiento de nuestros datos personales, lo legitima, y permite hablar de un mayor o menor control de los mismos, esto es, haber sido conscientes o no de que nuestros datos están siendo tratados». Cfr. M. Arenas Ramiro, «Refor-

mento jurídico más de entre los seis que relaciona el RGPD; ni siquiera es el principal, por mucho que ocupe el primer puesto en la lista que relaciona en su art. 6.

No obstante, con todo, es notorio que se trata de una pieza cardinal en la protección de datos que bien ha merecido un artículo específico en el Reglamento, fruto de la experiencia y de la intensa labor de estudio del grupo de trabajo creado por el art. 29 de la Directiva 95/46/CE (en adelante, GT29), pues cuando el fundamento jurídico del tratamiento es el consentimiento, este debe venir revestido de las garantías que resulten necesarias para considerar su licitud.

II. DE LA DEFINICIÓN DE CONSENTIMIENTO. SUS ELEMENTOS

El art. 4.11 RGPD nos ofrece una definición completa de lo que hemos de entender por la expresión *«consentimiento del interesado»* a los efectos de su aplicación:

> «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».

La Ley Orgánica 3/2018, de 5 de diciembre, sobre protección de datos personales y garantía de los derechos digitales, reproduce fielmente la definición en el apartado primero de su art. 6:

> «De conformidad con lo dispuesto en el art. 4.11 del Reglamento (UE) núm. 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».

Esta definición contiene una serie de elementos clave que analizaremos a continuación y que, como dijimos, suponen un importante refuerzo

---

zando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades», en A. Rallo Lombarte y R. García Mahamut (coords.), *Hacia un nuevo Derecho europeo de protección de datos,* 1.ª ed., Valencia, Triant lo Blanch, 2015, pp. 311-372, cita en la p. 329.

al consentimiento que exigía la derogada Directiva 95/46/CE y su correspondiente Ley Orgánica 15/1999.

1. Consentimiento inequívoco

Por un lado, se sigue hablando de «*toda manifestación de voluntad... mediante la que*», de modo que sigue admitiéndose una flexibilidad en la forma de emitir esa manifestación. Cualquier señal puede ser válida. En principio, y sin perjuicio de lo que diremos *infra* en relación con la «capacidad de demostrar» que pesa sobre el responsable, sirve tanto una declaración por escrito, inclusive por medios electrónicos, como una declaración verbal o una manifestación gestual, siempre que del comportamiento del interesado se deduzca razonablemente su consentimiento[10]. Si, por ejemplo, el decanato de una facultad universitaria comunica a los estudiantes que por la tarde tendrá lugar una sesión fotográfica en el aula X y que las imágenes que se seleccionen se utilizarán como material divulgativo de los servicios educativos del centro, invitando a los estudiantes que deseen participar en la campaña a presentarse en el aula X a la hora prevista, entenderemos que los estudiantes que han sido informados y deciden ir al aula señalada a la hora indicada consienten en ser fotografiados, pues están desplegando una acción afirmativa que inequívocamente manifiesta ese consentimiento. Por tanto, el quid no está en el medio o la forma en que se expresa el consentimiento, sino en la acción positiva que contiene la manifestación de voluntad: «*mediante una declaración o una clara acción afirmativa*».

Idéntico criterio ha de aplicarse a la participación de los usuarios en espacios públicos de internet como son los foros o *chat-rooms,* donde al facilitar voluntariamente sus datos de carácter personal, el usuario está autorizando de forma consciente e inequívoca su tratamiento para esta concreta finalidad (opinar en el foro), sin necesidad de marcar una casilla de consentimiento[11].

---

[10] Con una clara vocación didáctica y sin ánimo exhaustivo señala el considerando 32 del Reglamento que «esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales».

[11] Lo que deberá entenderse sin perjuicio del deber de informar que afecta a todo responsable en virtud de lo dispuesto en los arts. 13 y 14 RGPD, en relación con el art. 12 y el principio de transparencia consagrado en el art. 5.

Ahora bien, más allá de la forma en la que se manifieste la voluntad[12], el consentimiento inequívoco solo se podrá obtener cuando obedezca a una acción positiva, no pudiendo deducirse de la falta de respuesta de los afectados. A esta conclusión llega el GT29 en su Dictamen 15/2011, *sobre la definición del consentimiento*, al analizar, entre otros ejemplos, los parámetros de privacidad de una red social en la que los usuarios que no desean que su información personal sea vista por los «amigos de los amigos» tienen que marcar una casilla: «Es muy cuestionable que no marcar la casilla signifique que por lo general las personas consienten en que su información pueda ser vista por todos los "amigos de los amigos". Debido a la incertidumbre en cuanto a si la inacción significa consentimiento, el hecho de no marcar no puede considerarse consentimiento inequívoco»[13].

Atendiendo a estas consideraciones, el Reglamento nos reconduce a la necesidad de una posición activa del interesado que excluye la pasividad como manifestación del consentimiento tácito[14], es decir, inferido de la «falta de una manifestación contraria al tratamiento»[15]: la simple respuesta pasiva ya no es aceptada como manifestación de voluntad, especialmente en el contexto en línea[16]. Así, por ejemplo, si el espacio web de una tienda *online* que quiere fidelizar a sus clientes incluye una casilla con la leyenda

---

[12] En puridad, solo se exige el consentimiento explícito para el tratamiento de categorías especiales de datos personales [art. 9.2.*a)* RGPD], para las transferencias internacionales de datos (art. 49) o para la toma de decisiones individuales automatizadas, incluyendo *profiling* (art. 22), dado que, en estos contextos, el tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

[13] Dictamen 15/2011, de 13 de julio (WP 187), *On the definition of consent: «Example: default privacy settings. The default settings of a social network, which users do not necessarily need to access to use it, enable the entire "friends of friends" category making all the personal information of each user viewable to all "friends of friends". Users who do not wish to have their information viewed by "friends of friends" are required to click a button. If they remain passive, or fail to engage in the action consisting in clicking a button, they are deemed by the controller to have consented to having their data viewable. However, it is very questionable whether not clicking on the button means that individuals at large are consenting to have their information viewable by all the friends of friends. Because of the uncertainty as to whether the lack of action is meant to signify consent, not clicking may not be considered unambiguous consent».*

[14] Así se indica en el Preámbulo de la LOPDyGDD al señalar que «se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como "consentimiento tácito"».

[15] Giro importante en el consentimiento que, bajo la anterior legislación, avalaba el informe jurídico de la AEPD 93/2008, «Formas de obtener el consentimiento mediante web: consentimientos tácitos».

[16] El considerando 17 de la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, ha de entenderse en este mismo sentido cuando señala que: «El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre,

«he leído y consiento el tratamiento de mis datos personales», la casilla no podrá venir marcada por defecto, sino que, por el contrario, por defecto la casilla estará en blanco. Solo si el cliente marca la casilla tras haber recibido la información pertinente podrá entenderse que presta el consentimiento que requiere el RGPD para el tratamiento de sus datos en el programa de fidelización. De igual manera, quedan excluidas las casillas «no acepto» o «no quiero recibir publicidad» sin marcar[17].

Esto implica que todos aquellos consentimientos tácitos que se hayan obtenido en el marco de la Directiva 95/46/CE no se podrán beneficiar de la posibilidad que ofrece el considerando 171, que establece que cuando el tratamiento se base en el consentimiento obtenido de conformidad con la Directiva no será necesario recabar un nuevo consentimiento del interesado, siempre que este se ajuste a las condiciones del Reglamento. Cosa distinta es que, sometidos a revisión, se detecte para esos supuestos el acierto de otro fundamento jurídico distinto al consentimiento que sea el que realmente legitima el tratamiento[18]. En principio, en esta revisión habremos de dejar a un lado los supuestos enumerados en las letras *b)* a *e)* del art. 6.1 RGPD, pues, de otro modo, inicialmente no se habría recabado el consentimiento por no ser necesario[19]. En suma, habrá que examinar si los tratamientos basados en los consentimientos otorgados tácitamente bajo el man-

---

inequívoca y fundada de la voluntad del usuario, por ejemplo, mediante la selección de una casilla de un sitio web en internet».

[17] Considerando 32 RGPD: «Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento».

[18] Bien es cierto que el RGPD no permite pasar de una base jurídica a otra; sin embargo, sí se estima factible revisar el acierto de la base jurídica inicialmente identificada, máxime cuando el tratamiento está basado en el cumplimiento de una obligación legal o el responsable es una autoridad pública en el ejercicio de sus funciones, e inicialmente se invocó el consentimiento, siendo este, y para el caso concreto, un fundamento jurídico erróneo. Máxime teniendo en cuenta que, bajo el mandato de la LOPD de 1999, el consentimiento era la base legítima por excelencia, siendo las demás bases excepciones al criterio general. En todo caso, sobre la imposibilidad de pasar de una base jurídica a otra, *vid. Guidelines on consent under Regulation 2016/679,* último párrafo: *«Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable —as a one off situation— to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing».*

[19] Digo «en principio» porque pudiera ser que en el origen no se hubiera identificado correctamente la base jurídica del tratamiento, siendo este un buen momento para reconsiderar y definir la base de legitimación que corresponde. Insisto en que no se trata de pasar de una base jurídica a otra, sino de corregir un error para el que la interrupción del tratamiento no solo no se presenta como solución, sino que, además, podría ocasionar un incumplimiento legal o un trastorno grave a las funciones o intereses públicos.

dato de la Ley Orgánica 15/1999 pueden encontrar su base jurídica en el interés legítimo que consagra la letra *f)* del art. 6.1 RGPD[20], y, en su caso, si prevén garantías adecuadas para la salvaguarda de los derechos e intereses legítimos de los titulares de los datos, entre ellas un mecanismo viable que permita el ejercicio del derecho de oposición[21]. No se trata de pasar de una base jurídica a otra, sino de acertar en la asignación de la base jurídica para el tratamiento de datos personales con fines distintos pero compatibles con aquellos para los que se recogieron inicialmente, teniendo en cuenta, entre otras cosas, la relación entre los fines que motivaron la recogida de datos y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, la naturaleza del responsable, así como las expectativas razonables del interesado basadas en su relación con dicho responsable en los términos del considerando 50[22]. Si una vez hecha la debida ponderación establecida en el art. 6.1.*f)* RGPD no se aprecia la posibilidad de amparar el tratamiento en el supuesto del interés legítimo del responsable o del cesionario, será necesario recabar un nuevo consentimiento de los afectados que cumpla con los requisitos establecidos en el art. 4.11 RGPD.

Así, por ejemplo, de conformidad con el texto consolidado del art. 21.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, las encuestas de satisfacción y el ofrecimiento de productos y servicios realizados por una empresa a sus clientes en relación con productos y servicios objeto de una relación previa de carácter contractual podrán amparar el tratamiento de datos en el interés legítimo basado en una relación contractual anterior, teniendo en cuenta las expectativas razonables y previa su correspondiente ponderación con los derechos y libertades de los interesados, que deberá quedar

---

[20] Art. 6.1.*f)* RGPD: «El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño».

[21] *Vid.*, en este sentido, el Informe 195/2017 de la AEPD, en el que se elabora un interesante análisis del interés legítimo que ahora aborda el art. 6.1.*f)* RGPD, y el Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del art. 7 de la Directiva 95/46/CE, adoptado por el GT29 el día 9 de abril de 2014.

[22] En torno a las bases jurídicas del tratamiento, *vid.* los comentarios a los arts. 6 RGPD y 8 LOPDyGDD y disposición adicional duodécima de la LOPDyGDD, de J. Sempere Samaniego, «La licitud del tratamiento», en A. Troncoso Reigada (dir.) y J. J. González Rivas (pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos,* vol. I, 1.ª ed., Pamplona, Civitas, 2021, pp. 925-944.

documentada[23]. Motivo por el que no será necesario dirigirse a los clientes/destinatarios para recabar un consentimiento acorde con el RGPD.

Por último, interesa destacar que, al comentar este requisito, deliberadamente he evitado utilizar el término «expreso», que bien podría haber empleado en contraposición al adjetivo «tácito» que se aplica a aquel consentimiento que no se percibe, oye o dice formalmente, pero que se supone e infiere. Enfatizo este extremo con la intención de evitar la confusión con los supuestos tasados en los que el RGPD verdaderamente exige el consentimiento expreso o explícito —según como se traduzca el término *«explicit»*— referidos al tratamiento de categorías especiales de datos personales (art. 9); a las decisiones basadas únicamente en el tratamiento automatizado de datos personales, incluida la elaboración de perfiles [art. 22.1.*c)*], y a la transferencia internacional de datos a terceros países u organizaciones internacionales cuando no haya nivel adecuado de protección (art. 49). De hecho, el GT29, en sus Directrices sobre el consentimiento conforme al Reglamento 2016/679[24], distingue entre el consenti-

---

[23] En línea con lo dispuesto en el art. 13 de la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, el art. 21 de Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), regula como regla general la prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas, si bien en su apartado 2.º introduce una salvedad a esta prohibición, con sus condiciones:

«2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección».

Por su parte, el art. 38 LSSI califica como infracción grave «el envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos establecidos en el art. 21», rebajando a infracción leve «el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el art. 21 y no constituya infracción grave».

[24] *Guidelines on Consent under Regulation 2016/679* (WP 259): *«The GDPR prescribes that a "clear affirmative act" is a prerequisite for "regular" consent. As the "regular" consent*

miento normal o *«"regular" consent»* y el consentimiento explícito que se presta como medida reforzada en el control del interesado sobre sus datos personales ante los supuestos que entrañan un alto riesgo para la protección de los datos personales.

2. Consentimiento libre

La manifestación de voluntad ha de ser «libre». Es decir, deberá haber sido obtenida sin la presencia de vicio alguno del consentimiento en los términos regulados por el Código Civil[25]. El consentimiento libre supone una decisión voluntaria tomada por un individuo que está en posesión de todas sus facultades, adoptada sin ningún tipo de coacción, ya sea social, financiera, psicológica u otra[26]. Implica control sobre la propia información: libertad por parte del titular para autorizar o retirar esa autorización otorgada para el tratamiento de sus datos sin que pueda verse perjudicado por una posterior rectificación en el consentimiento otorgado. Si el sujeto no tiene esa verdadera libertad para gestionar su propia información personal no puede decirse que el consentimiento sea libre. Así lo señala el considerando 42:

> «El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno».

---

requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the explicit consent of a data subject in line with the GDPR.

The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future» (texto adoptado el 28 de noviembre de 2017).

[25] Art. 1265 CC: «Será nulo el consentimiento prestado por error, violencia, intimidación o dolo».

[26] Documento del GT29, *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (WP 131), p. 8: *«Consent must be given freely: "Free" consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as "free". Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a fait accompli cannot be considered to be valid»* (texto adoptado el 15 de febrero de 2007).

En el Dictamen WP 131, el GT29 aclara que no se puede considerar válido el consentimiento dado por un interesado que no haya tenido la oportunidad de hacer una verdadera elección so pena de sufrir un perjuicio o que se haya encontrado frente a un hecho consumado[27]: «El consentimiento dado bajo amenaza de no tratamiento o de tratamiento de menor calidad en una circunstancia médica no puede considerarse "libre"»[28]. Es importante tener en cuenta que el RGPD no excluye los incentivos, pero estos no deben ser de tal naturaleza que anulen la verdadera libertad. En todo caso, recae sobre el responsable la carga de demostrar que el consentimiento que se obtuvo fue válido y, por tanto, libre.

2.1. *Desequilibrio de poder*

El considerando 43 completa lo que hemos de entender por consentimiento libre y aclara que no se puede aplicar el fundamento jurídico del consentimiento cuando en el caso concreto exista un desequilibro claro entre el interesado y el responsable del tratamiento, como normalmente sucede, por ejemplo, en los tratamientos llevados a cabo por las autoridades públicas, donde resulta improbable que el consentimiento se haya dado libremente, ya sea por la situación de predominio sobre el titular de los datos o bien porque la prestación del servicio público pretendido requiere inevitablemente el tratamiento de los datos personales[29]. En estos casos, deberá buscarse la legitimación del tratamiento en otro fundamento jurídico, pues no concurre la libertad del consentimiento y, por tanto, no resulta válido a estos efectos. De hecho, habitualmente en estos supuestos, el tratamiento o bien está justificado en una norma con rango de ley [art. 6.1.*c)* RGPD] o bien halla su legitimación en el cumplimiento de una

---

[27] *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (WP 131), apartado II.4: «*Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a "fait accompli" cannot be considered to be valid... Reliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment*» (texto adoptado el 15 de febrero de 2007).

[28] Dictamen 8/2001, de 13 de septiembre de 2001 (WP 48), *On the processing of personal data in the employment context.*

[29] Considerando 43 RGPD: «Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea, por tanto, improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular».

misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento [art. 6.1.*e)* RGPD], aunque en este caso se precisará igualmente una norma habilitante que confiera tanto el interés público a dicha misión como el ejercicio del poder público de tal función. Por ejemplo, el tratamiento de los datos personales del nivel de renta y condiciones familiares de los beneficiarios de una beca convocada por el Ministerio de Educación, Cultura y Deporte no estará basado en el consentimiento de los estudiantes, por mucho que estos hayan solicitado voluntariamente la beca, pues aquellos que deseen concurrir al procedimiento competitivo no tienen una alternativa real, dado que el Ministerio está obligado a tratar tales datos conforme a lo dispuesto en la Ley General de Subvenciones y en la propia convocatoria, de acuerdo con la normativa por la que se establecen los umbrales de renta y patrimonio familiar, y sin perjuicio de la posible concurrencia de otras normas con rango de ley como pueden ser la Ley del Procedimiento Administrativo Común o la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, y demás normas sectoriales.

No obstante, no debe descartarse de forma absoluta el consentimiento en el contexto de la autoridad pública. De hecho, en determinadas circunstancias el uso del consentimiento puede resultar adecuado. El GT29 presenta varios ejemplos prácticos de consentimiento otorgado válidamente por los particulares para el tratamiento de sus datos personales por las autoridades públicas[30].

Lo mismo cabe señalar del entorno laboral, donde concurre una dependencia del empleado con respecto del empleador (o responsable) susceptible de generar consecuencias negativas en la esfera del trabajador si no consiente el tratamiento de sus datos, por lo que, como regla general, resulta inapropiado basar en el consentimiento la legitimación para el tratamiento de los datos de los empleados en el entorno labo-

[30] *Guidelines on Consent under Regulation 2016/679* (WP 259), apartado 3.1.1. Entre ellos, resulta esclarecedor el siguiente ejemplo: «Un municipio está planificando obras de mantenimiento vial. Dado que dichas obras pueden perturbar el tráfico durante mucho tiempo, el municipio ofrece a sus ciudadanos la oportunidad de suscribirse a una lista de correo electrónico para recibir información actualizada sobre el progreso de las obras y las demoras previstas. El municipio deja claro que no existe la obligación de participar y pide el consentimiento para utilizar las direcciones de correo electrónico para este (exclusivo) fin. Los ciudadanos que no dan su consentimiento no se ven privados de ningún servicio básico del municipio ni del ejercicio de ningún derecho, por lo que tienen la capacidad de dar o negar libremente su consentimiento para este uso de sus datos. La información sobre las obras estará también disponible en el sitio web del municipio».

ral[31]. Ahondando algo más en el contexto del empleo, el documento de trabajo sobre la vigilancia de las comunicaciones electrónicas en el lugar de trabajo (WP 55) resalta que los correos electrónicos contienen datos personales tanto del remitente como del destinatario, por lo que habitualmente a los empleadores les resultará complicado obtener el consentimiento de ambos intervinientes —salvo que se trate de correspondencia interna—, de donde concluye que la legitimación para la supervisión de los correos electrónicos sobre la base del consentimiento es muy limitada. En este contexto, el GT29 invoca el Dictamen 8/2001 para recordar que el consentimiento de los trabajadores debe darse libremente y plenamente informado, y los empleadores no deben confiar en el consentimiento de sus empleados como un medio adecuado para legitimar la supervisión del correo electrónico de los trabajadores, precisamente por ese desequilibrio que preside la relación entre ellos. Así las cosas, argumenta el GT29, la legitimación más probable para este tratamiento puede encontrarse en el art. 7.*f)* de la Directiva 95/46/CE, es decir, en el interés legítimo perseguido por el empleador o por el tercero o las partes a quienes se comuniquen los datos, si bien matiza que esa legitimación no puede anular los derechos y libertades fundamentales del trabajador. Insiste, en suma, en la prevalencia del derecho fundamental al secreto de la correspondencia, salvo en circunstancias muy especiales y limitadas que justifiquen esa intervención del empleador sobre la comunicación personal de sus empleados[32].

En idéntico sentido se pronuncia el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (WP 249), que nuevamente y como regla general descarta el consentimiento como base jurídica que legitime la observación del empresario sobre las comunicaciones electrónicas y el uso de internet de sus trabajadores, esencialmente por el desequilibrio de poder inherente a la relación entre las partes, donde los trabajadores casi nunca están en condiciones de dar, denegar o revocar ese consentimiento libremente, habida cuenta de la dependencia que resulta de la relación empresario/trabajador. En consonancia con lo expuesto, y sin des-

[31] Muy interesante, J. Baz Rodríguez, «Protección de datos y garantía de los derechos digitales laborales en el nuevo marco normativo europeo e interno (RGPD 2016 y LOPDP-GDD 2018)», *Ars Iuris Salmanticensis (AIS): Revista europea e iberoamericana de pensamiento y análisis de Derecho, ciencia política y criminología,* vol. 7, núm. 1 (2019), pp. 129-171, esp. p. 156. *Vid.,* asimismo, el Dictamen 8/2001, de 13 de septiembre (WP 48), *On the processing of personal data in the employment context*.

[32] *Working document on the surveillance of electronic communications in the workplace* (WP 55), apartado 4.2, adoptado el 29 de mayo de 2002.

cartar la posible presencia de un interés legítimo del empresario, acentúa la conveniencia de realizar una prueba de proporcionalidad antes de la utilización de cualquier herramienta de observación de los trabajadores basándose en la letra *f)* del art. 7 de la Directiva, equivalente al actual art. 6 RGPD. Considerando, pues, que el interés legítimo de los empresarios puede invocarse en ocasiones como fundamento jurídico, recalca, no obstante, la prevalencia del secreto de las comunicaciones como punto de partida necesario[33].

Interesa destacar que en este contexto pueden coexistir variados fundamentos jurídicos que legitimen el tratamiento de los datos. Así, por ejemplo, se aplicará el art. 6.1.*b)* para el tratamiento de datos que tenga por objeto el desempeño de las funciones del empleado; el art. 6.1.*c)* para el tratamiento del número de afiliación a la seguridad social, o el art. 6.1.*f)* para el tratamiento de datos de geolocalización en vehículos de empresa durante la jornada laboral[34], mientras que el consentimiento se limitará a legitimar el tratamiento en aquellos supuestos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad real de retirar posteriormente su consentimiento sin perjuicios derivados de esta rectificación, como puede ser la suscripción de opciones sobre acciones o participación en un plan de *stock options*[35].

---

[33] Dictamen 2/2017 (WP 249), *On data processing at work*, apartado 6.2, adoptado el día 8 de junio de 2017.

[34] Expresamente el considerando 47 alude a un posible supuesto del art. 6.1.*f)* en los casos en que existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado está al servicio del responsable.

En relación con el ejemplo propuesto, se recomienda la lectura de la STSJ de Asturias (Sala de lo Social, Sección 1.ª) de 27 diciembre (asunto 2018\296).

[35] Dictamen 15/2011, de 13 de julio (WP 187), *On the definition of consent:*

«Data necessary for the exercise of its tasks by the employee: application of article 7.b) *—necessity for the contract—.*

To determine employees' entitlement to acquire stock options: it could either be on the basis of consent —article 7.a)*—, or considered as inherent to the administrative aspects of the contractual work relationship —article 7*.b)*—.*

Processing the social security number for social security purposes: article 7.c) *—legal obligation—, or possibly article 8*.b) *—obligations in the field of employment law—.*

Processing of ethnic data: in some countries, this could also be an obligation due to employment law —article 8.b)*—, while in other countries it would be strictly forbidden».*

2.2. *La ejecución de un contrato supeditada al consentimiento*

El considerando 43 entiende, asimismo, que el consentimiento no es libre si el sistema o el procedimiento arbitrado al efecto no permite autorizar por separado las distintas operaciones de tratamientos de datos personales previstas, aun a pesar de que sea adecuado para el caso concreto[36]. Avanzando en esta misma línea, se presume que el consentimiento no se ha prestado libremente cuando el cumplimento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento (art. 7.4 RGPD).

Esta presunción que incorpora el considerando sugiere, ya de antemano, un análisis de cada caso concreto, que se ratifica en el cuerpo del articulado con la expresión «tener en cuenta en la mayor medida posible», que presenta el apartado 4 del art. 7 RGPD; si bien ambos enunciados proclaman una clara excepcionalidad, dejando un espacio muy limitado a los supuestos en los que dicha condicionalidad no invalidaría el consentimiento.

De forma algo más contundente se pronuncia el apartado 3 del art. 6 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDyGDD) al disponer que:

> «No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual».

La revisión de los preceptos señalados a la luz del considerando 43 nos obliga a analizar la presencia de esa «necesidad» de los tratamientos de datos que se establecen en el clausulado como requisito para la ejecución del contrato.

Respecto a lo que hemos de entender por «necesario», el GT29 aclara que «el hecho de que el tratamiento de algunos datos esté cubierto por un contrato no quiere decir automáticamente que el tratamiento sea necesario para su ejecución [...]. Incluso si estas actividades de tratamiento se mencionan de manera específica en la letra pequeña del contrato, este hecho por sí solo no las convierte en "necesarias" para la ejecución del contrato». Y añade que «existe una clara relación entre la valoración de la necesidad

[36] Cuestión que analizaremos con más detalle al revisar el consentimiento «específico».

y el cumplimiento del principio de limitación de la finalidad. Es importante determinar la justificación exacta del contrato, es decir, su esencia y objetivo fundamental, ya que la evaluación para comprobar si el tratamiento de datos es necesario para su ejecución se realizará en función de esta información»[37].

En consecuencia, define un criterio de interpretación estricta que deberá atender a la existencia de un vínculo directo y objetivo entre el tratamiento pretendido y la finalidad del contrato. En caso de existir ese vínculo real, la base jurídica del tratamiento no será el consentimiento, sino el contrato, contemplado en la letra *b)* del art. 6 RGPD.

Por el contrario, si se descarta la necesidad del tratamiento, pero su previsión está incluida como una parte no negociable de las condiciones generales de un contrato, se entiende *prima facie* que dicho tratamiento ha sido impuesto unilateralmente al interesado por parte del responsable y, por consiguiente, el consentimiento no se ha prestado libremente. No obstante, y en aras de aquella presunción que anuncia el considerando 43, deberá examinarse cada supuesto concreto, pues nada impide que se presenten situaciones complejas en las que, efectivamente, el responsable facilite al interesado dos modelos de contrato o prestación de servicio equivalentes, incluyéndose en uno de los dos modelos a elegir libremente fines adicionales para los que el interesado consiente el uso de sus datos, sin merma de la prestación del servicio o de la ejecución del contrato para el supuesto de elección del modelo «básico».

Con esta previsión pretende evitarse que el tratamiento camuflado al hilo de una relación contractual con la que no guarda verdadera relación se convierta, en la práctica, en la contraprestación de dicho contrato. Y a este tenor, las dos bases jurídicas para el tratamiento lícito de los datos personales, a saber, el consentimiento y el contrato, no pueden fusionarse[38]. El GT29 ilustra el supuesto sobre el siguiente ejemplo:

> «Una aplicación de móvil para edición de fotografías solicita a sus usuarios que tengan activada su localización GPS para el uso de sus servicios. La aplicación también avisa a sus usuarios que usará los datos recabados para fines de publicidad comportamental. Ni la geolocalización ni la publicidad comportamental son necesarias para la prestación del servicio de edi-

[37] Dictamen 06/2014 (WP 217), *On the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, apartado III.2.2, adoptado el 9 de abril de 2014.

[38] Sobre todo esto y lo que sigue, *vid. Guidelines on Consent under Regulation 2016/679* (WP 259), ya citado.

> ción de fotografías y van más allá de lo necesario para prestar el servicio básico ofrecido. Dado que los usuarios no pueden utilizar la aplicación sin dar su consentimiento a estos fines, no puede considerarse que el consentimiento se haya otorgado libremente».

De igual manera, el acceso a los servicios de redes sociales no podrá condicionarse a la prestación de un consentimiento para recibir publicidad comportamental, pues esta condición anularía la libertad requerida para la prestación del consentimiento válido.

Por tanto, y resumiendo, en términos generales, el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado que impida que este manifieste su íntima voluntad. Para que el consentimiento sea libre, el interesado deberá encontrarse en la situación real de poder elegir si autoriza el tratamiento de sus datos o no, sin que la negativa a dar el consentimiento o su posterior retirada pueda causarle perjuicios. De tal suerte, para que el consentimiento se considere libre habrá de estar debidamente informado y se manifestará de forma separada e independiente a la firma del contrato y aceptación de un servicio[39]. En otro caso, se estará presentando al individuo una falsa ilusión del control de sus datos[40].

2.3. *La retirada del consentimiento*

Dice el considerando 42 que:

> «El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno».

Por tanto, la posibilidad de retirar el consentimiento es considerada por el RGPD como uno de los requisitos necesarios para que concu-

---

[39] El considerando 25 de la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, advierte que: «La presentación de la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante, se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un "chivato" *(cookie)* o dispositivo similar, en caso de que este tenga un propósito legítimo».

[40] «*It presents the individual with a false choice and only the illusion of control*». Así en Information Comissioner's Office (ICO), «Consultation: GDPR consent guidance», 2 de marzo de 2017, disponible en *https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.*

rra el elemento de la libertad, y, por tanto, se configura como una condición necesaria para la validez del consentimiento. Hasta tal punto es así que lo que en la Ley Orgánica 15/1999 no era más que una posibilidad sujeta a condición[41], en el art. 7.3 del Reglamento se eleva a categoría de «derecho»:

> «El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo».

El derecho a retirar el consentimiento se alinea con la naturaleza de derecho fundamental atribuida a la protección de datos, toda vez que constituye un bastión esencial de la capacidad de cada persona de controlar los datos personales que le conciernen[42]. Y por eso, y en tal medida, cuando la base jurídica que legitima el tratamiento es el consentimiento, el interesado tiene derecho a revocar el consentimiento anteriormente otorgado. De otro modo, se estaría viciando la libertad de elección de la persona.

Para que este derecho sea cierto, el responsable deberá informar al interesado en el momento de la recogida de los datos de la posibilidad de retirar su consentimiento en cualquier momento y sin necesidad de justificación alguna. En definitiva, retirar el consentimiento será tan sencillo como otorgarlo. Además, y como quiera que el ejercicio de este derecho no puede imponer condiciones gravosas que impidan o dificulten la decisión de revocación, el responsable deberá arbitrar un procedimiento sencillo y gratuito que permita hacer efectiva esta opción, quedando obligado a poder demostrar que la retirada del consentimiento no conlleva ningún

---

[41] Art. 6.3 de la Ley Orgánica 15/1999, de 13 de diciembre: «3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos».

[42] Es importante no perder de vista la declaración de intenciones que contiene el considerando 2, cuyo contenido preside la formulación de todo el Reglamento: «Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia, y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas».

coste para el interesado ni merma alguna en la prestación del servicio ni, en definitiva, conlleva ninguna clara desventaja.

Solo cumpliendo estos presupuestos, el interesado mantiene el poder de disposición y control sobre sus datos en todo momento.

En todo caso, la revocación del consentimiento no tiene efecto retroactivo, por lo que esta decisión no alterará la licitud del tratamiento fundamentado en el consentimiento prestado con anterioridad a la revocación.

3. Consentimiento específico

La manifestación de voluntad ha de ser, además, «específica», como garantía de un apreciable nivel de control y transparencia sobre los datos personales. Esta especificidad significa que el consentimiento ha de venir referido a una (o unas) determinada(s) operación(es) de tratamiento y para una (o unas) determinada(s) y legítima(s) finalidad(es) del responsable del tratamiento. En la base de este elemento se encuentran los principios de licitud, transparencia, lealtad, limitación de la finalidad y minimización de datos[43]. De modo que será esencialmente injusta la recogida de datos personales que no sean necesarios para el fin concreto que el interesado consintió y del mismo modo que será ilícito el tratamiento efectuado sin un consentimiento específico en relación con la finalidad legítima y explícita que lo ampare.

Por tanto, y como punto de partida, el responsable deberá identificar cuidadosamente el fin o los fines del tratamiento, quedándole prohibida la recopilación de datos personales que no resulten necesarios, adecuados o relevantes para los fines pretendidos, aunque consienta la persona concernida.

De igual manera, la limitación de la finalidad vinculada al consentimiento específico requiere una disociación de los fines. No se admite el consentimiento otorgado para un fin tan vago o general que, en la práctica, suponga un riesgo para los derechos y libertades de las personas físicas, por dar cobertura a un universo de posibilidades para usos imprevistos de los datos con los que no contaba la persona concernida[44]. Si bien, y como subraya el GT29, no siempre es más precisa la información más larga

[43] Art. 5.1.*a), b)* y *c)* RGPD.

[44] Es el caso de enunciados como «mejorar la experiencia del usuario», «fines de mercadotecnia», «fines de seguridad informática» o «futuras investigaciones».

o más detallada con respecto a especificaciones inútiles, máxime cuando se introducen términos especialmente legalistas y farragosos que, en lugar de ayudar, pueden confundir al lector[45].

En el documento (WP 259) relativo a las directrices sobre el consentimiento conforme al Reglamento 2016/679, el GT29 parte del hecho de que un servicio puede implicar múltiples actividades de tratamiento para más de una finalidad. En una situación así, los titulares de los datos deben poder decidir qué finalidad o qué finalidades aceptan de todas las propuestas, sin que un único consentimiento pueda implicar el de una multitud de tratamientos con finalidades distintas. Tal criterio parece deducirse claramente de los considerandos 32 y 43 RGPD:

> Considerando 32: «El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos».
>
> Considerando 43: «Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto».

Así, por ejemplo, el consentimiento dado para el tratamiento de datos personales con la finalidad de descarga en un ordenador de una aplicación gratuita no puede ser utilizado para la elaboración del perfil del usuario sobre sus preferencias y transacciones[46]. Como tampoco el acceso a los servicios de redes sociales puede condicionarse a la prestación de un consentimiento para recibir publicidad comportamental, pues el usuario debe

---

[45] Dictamen 3/2013 (WP 203), *On purpose limitation*, apartado III.1.1, adoptado el 2 de abril de 2013.

[46] Para valorar estos criterios en su justa medida debemos tener en cuenta el Dictamen 4/2007 del GT29, donde se advierte que: «En Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones, puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos. La definición de datos personales refleja este hecho». *Vid.* Dictamen 4/2007 (WP 136), *On the concept of personal data*, adoptado el 20 de junio de 2007.

estar en condiciones de prestar su consentimiento libre y específico para recibir publicidad comportamental, independientemente de su acceso al servicio de la red social. El GT29 propone la utilización de ventanas desplegables que proporcionen la posibilidad real de seleccionar el uso de los datos para el que el interesado da su consentimiento (transmisión al promotor, servicios de valor añadido, publicidad comportamental, transmisión a terceros, etc.)[47].

De ahí que el precitado considerando 43 presuma que el consentimiento no se ha dado libremente cuando el procedimiento establecido para recabar el consentimiento no permita disociar las finalidades y, en consecuencia, autorizar por separado las distintas operaciones de tratamientos de datos personales, pese a ser adecuados en el caso concreto. De este modo, y avanzando con el ejemplo anterior, si la finalidad con la que se recogen los datos es la suscripción a un periódico electrónico, los datos del usuario no podrán utilizarse para la captación de hábitos de navegación y consumo con la finalidad de envío de publicidad personalizada, salvo que medie un nuevo y específico consentimiento, que además habrá de manifestarse de forma afirmativa, como contraposición al consentimiento tácito que se admitía antes del 25 de mayo de 2018.

Sin embargo y a la inversa, un único consentimiento puede ser suficiente para legitimar varios tratamientos con una misma finalidad, siempre y cuando el interesado haya sido debidamente informado en el momento del primer tratamiento y la finalidad no varíe en los tratamientos posteriores[48]. Y en ambos sentidos, el considerando 32 dispone que:

> «El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos».

En suma, y como criterio general, habrá de considerarse suficiente que los responsables del tratamiento recaben una sola vez el consentimiento para todas las operaciones, siempre que estas respondan a la misma finalidad y el consentimiento esté debidamente informado[49]. Sin embargo, y por

---

[47] Dictamen 15/2011, de 13 de julio (WP 187), ya citado.

[48] *Vid.* Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera) de 5 de mayo de 2011 (TJCE 2011\120), asunto C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland.*

[49] En este sentido, la Directiva 2002/58 sobre la privacidad y las comunicaciones electrónicas establece, con respecto a las guías públicas en las que figuren datos personales de los abonados a un número de teléfono, la obligación de la empresa que recoja estos

el contrario, se entiende que no hay libertad si el responsable ha decidido varias finalidades para el tratamiento y no ha recabado el consentimiento específico para cada fin.

En muchos casos, y cuando las finalidades sean independientes unas de otras, la aplicación de este criterio no planteará dudas. Así, por ejemplo, se considera ilícita la recopilación de datos procedentes de espacios públicos de internet, tales como directorios públicos, foros o redes sociales, en los que el interesado no dio con su mera participación otro consentimiento que el de su intervención en dichos espacios[50].

Ahora bien, frente a estos supuestos deben valorarse otras situaciones en las que las finalidades, aun siendo distintas, están relacionadas entre sí. En estos casos, la duda se plantea en torno a la obligación del responsable de especificar los detalles de cada una de tales finalidades de cara a la obtención de un consentimiento específico para cada una de ellas. El GT29 aprecia esta situación y estima la posibilidad de enunciar un fin general que aglutine todas las operaciones de tratamiento «relacionadas». Si bien alerta de que no podrá utilizarse esta posibilidad para legitimar actividades de tratamientos de datos adicionales, que de hecho solo están remotamente relacionadas con la verdadera finalidad inicial[51].

---

datos de informar a los titulares acerca de los objetivos de dichas guías. Además, señala su considerando 39 que cuando los datos puedan ser transmitidos a una o más terceras partes, deberá informar al abonado de esta posibilidad, así como acerca del destinatario o de las categorías de posibles destinatarios; si bien cualquier transmisión debe estar sujeta a la condición de que los datos no puedan utilizarse para otros fines distintos de aquellos para los que se recojan, de modo que si quien recoge datos del usuario o cualquier tercero a quien se hayan transmitido los datos desea utilizarlos con un fin suplementario, será preceptiva la renovación del consentimiento del abonado. El TJUE ha sentenciado que dicha transmisión no está supeditada a un nuevo consentimiento de los abonados, siempre y cuando estos hayan sido informados, antes de la primera inclusión de sus datos en una guía pública, de la finalidad de esta y del hecho de que sus datos podrían ser comunicados a otro proveedor de servicios telefónicos, siempre que se garantice que, tras la transmisión, los datos no puedan utilizarse con fines distintos de aquellos para los que se hayan recogido para su primera publicación. Así en SSTJUE de 15 de marzo de 2017, *Tele2 (Netherlands) y otros,* asunto C-536/15, y de 5 de mayo de 2011, *Deutsche Telekom c. Alemania,* asunto C-543/09.

[50] El GT29 concluye que si una dirección de correo electrónico se obtiene en un espacio público de Internet, su utilización para envíos comerciales electrónicos constituiría un tratamiento «desleal» de los datos personales; sería contraria al principio de la finalidad, ya que el interesado proporcionó su dirección de correo electrónico para una finalidad muy distinta, como puede ser la participación en un foro, por ejemplo, y dado el desequilibrio del coste y la interrupción para el destinatario, se puede considerar que estos envíos no superarían la prueba del equilibrio de intereses. *Vid.* Dictamen 1/2000, de 3 de septiembre (WP 28), *On certain data protection aspects of electronic commerce.*

[51] Dictamen 3/2013 (WP 203), *On purpose limitation*, ya citado, apartado III.1.1.

En el mismo orden de cosas, y a partir del análisis de estos considerandos en relación con los arts. 4.11 y 7 RGPD, el GT29 enfatiza la importancia de que las finalidades del tratamiento sean específicas de acuerdo con el requisito de «granularidad» y no puedan diluirse una vez que el sujeto ha consentido a la recogida de datos, en lo que denomina el riesgo de «desviación de uso» *(function creep)*[52].

De tal suerte, el actual panorama legal no admite el consentimiento otorgado de forma indiscriminada para una multitud de finalidades[53], sino que deberán proporcionarse opciones de «consentimiento granular» o «vertebrado» que permitan a los titulares de los datos consentir por separado los tratamientos objeto de distintas finalidades; obviamente, en la medida en que esos tratamientos no sean necesarios para la prestación del servicio en el que se registra o que solicita[54]. El apartado 2 del art. 6 LOPDyGDD es claro al respecto:

> «Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas»[55].

Estas «vértebras» o dosis de consentimiento van a permitir al usuario del sistema entender las circunstancias y la finalidad del consentimiento

---

[52] *Guidelines on Consent under Regulation 2016/679* (WP 259).

[53] Si bien el GT29 subraya que este requisito no es una novedad del RGPD, lo cierto es que la derogada LO 15/1999 hablaba tan solo de un «consentimiento inequívoco del afectado».

[54] En este sentido, el considerando 22 de la Directiva 2002/58/CE, sobre privacidad y comunicaciones electrónicas, aclara que: «Al prohibirse el almacenamiento de comunicaciones, o de los datos de tráfico relativos a estas, por terceros distintos de los usuarios o sin su consentimiento no se pretende prohibir el almacenamiento automático, intermedio y transitorio de esta información, en la medida en que solo tiene lugar para llevar a cabo la transmisión en la red de comunicaciones electrónicas, y siempre que la información no se almacene durante un periodo mayor que el necesario para la transmisión y para los fines de la gestión del tráfico, y que durante el periodo de almacenamiento se garantice la confidencialidad».

[55] El proyecto de ley orgánica señalaba que «dicho consentimiento se otorga para cada una de ellas», optando de este modo por una dimensión tal vez demasiado estricta del consentimiento específico. El Grupo Parlamentario Ciudadanos, al presentar la enmienda núm. 5 de modificación del apartado 2 del art. 6 del Proyecto de Ley Orgánica, propuso sustituir la fórmula «para cada una de ellas» por «para todas ellas», argumentando que «el RGPD, en su considerando 32, parece ser más flexible al establecer que, en estos supuestos, "el consentimiento debe darse para todos ellos", en lugar de tener que realizar un ejercicio particularizado y específico finalidad a finalidad». En la misma línea, el Grupo Parlamentario Socialista presentó enmienda de modificación núm. 252, por la que proponía sustituir al final del apartado 2 los términos «cada una de ellas» por «todas ellas», alegando lacónicamente la «mejora técnica y en coherencia con el contenido del Reglamento».

que se le requiere en cada momento, por lo que el interesado podrá valorar de forma intuitiva si lo que se le pide está justificado para el producto o servicio que desea obtener. Sucede, además, que las vértebras o permisos están conectados entre sí, de modo que se le deberá presentar al usuario, de forma clara y transparente, que es posible que la denegación de algún permiso le impida el acceso o alguna de las prestaciones del servicio, o un conjunto de ellas. Con este requisito se pretende un mayor grado de control del usuario sobre sus datos, en una relación íntimamente vinculada a la transparencia de la información[56], que en la práctica tendrá enorme relevancia a la hora de diseñar los procedimientos y habilitar las casillas para recabar el consentimiento en línea o bien idear otras formas de obtenerlo.

De otro lado, la especificidad que se le requiere al consentimiento significa también que, si los fines para los que el responsable trata los datos cambian o se amplían en algún momento, el usuario deberá ser informado y estar en condiciones de dar su consentimiento para el nuevo tratamiento de los datos[57].

4. Consentimiento informado

En estrecho maridaje con los principios del tratamiento lícito, leal y transparente, la manifestación de voluntad debe ser «informada».

El considerando 42 analiza al detalle los vericuetos de este aspecto del consentimiento:

> «En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es cons-

[56] *«The requirement that consent must be "specific" aims to ensure a degree of user control and transparency for the data subject».*

[57] En este mismo sentido se pronuncia el considerando 39 de la Directiva 2002/58/CE respecto al consentimiento otorgado por los interesados para la inclusión de sus datos personales en las guías de abonados a los servicios de comunicaciones electrónicas y para el supuesto de que los datos puedan ser transmitidos a una o más terceras partes, en cuyo caso, además del deber de informar al abonado de esta posibilidad, así como acerca del destinatario o de las categorías de posibles destinatarios, aclara la Directiva que: «Cualquier transmisión debe estar sujeta a la condición de que los datos no puedan utilizarse para otros fines más que aquellos para los que se recojan. Si quien recoge datos del usuario o cualquier tercero a quien se hayan transmitido los datos desea utilizarlos con un fin suplementario, la renovación del consentimiento del abonado deberá obtenerla ya sea quien recogió inicialmente los datos o el tercero a quien se hayan transmitido».

> ciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo[58], debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales».

El considerando 60 precisa que debe informarse al interesado de la existencia de una operación de tratamiento y sus fines, junto a la obligación del responsable de facilitar al interesado cuanta información complementaria sea necesaria para garantizar el tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Además, se debe informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Asimismo, si los datos personales se obtienen de los interesados, se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. También el considerando 39 especifica que debe quedar totalmente claro para las personas físicas que se están recogiendo, utilizando, consultando o tratando de otra manera sus datos personales, así como la medida en que dichos datos son o serán tratados[59].

---

[58] Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (*DO,* núm. L 95, de 21 de abril de 1993, p. 29).

[59] Considerando 39 RGPD: «Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiem-

Es suma, el interesado debe poder saber con anterioridad al tratamiento qué datos suyos se van a utilizar, para qué (finalidad) y quién los va a tratar (identidad del responsable).

Por su parte, los arts. 13 y 14 RGPD[60] enfatizan el deber de transparencia que sanciona el art. 12, regulando la información que se debe proporcionar a las personas interesadas en relación con los tratamientos que se pretenden llevar a cabo sobre los datos que les conciernen[61].

El RGPD no limita la forma en la que debe darse esa información, de modo que habremos de entender que se utilizará un medio adecuado a la forma de prestar el consentimiento, siendo válidas las locuciones verbales, los mensajes de audio o vídeo, las declaraciones escritas o cualquier otro medio que se estime oportuno. Sin embargo, en todo caso, esa información debe presentarse de forma clara y concisa, empleando un lenguaje sencillo de entender que evite estructuras lingüísticas complejas[62] y que sea de fácil acceso para el destinatario/interesado[63]. En esta línea y para el caso de información «escrita», más allá de los métodos de transcripción Braille y dependiendo de la situación concreta en que se requiera el consentimien-

---

po del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento».

[60] Sobre esto *vid.* M. Arias Pou, «Transparencia e información que deberá facilitarse cuando los datos personales se obtengan del interesado. El derecho a la información desde el diseño (comentario al art. 13 RGPD y al art. 11.1 y 2 LOPDyGDD)», en A. Troncoso Reigada (dir.) y J. J. González Rivas (pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos,* vol. I, 1.ª ed., Pamplona, Civitas, 2021, pp. 1357-1379.

[61] *Vid. Guidelines on Transparency under Regulation 2016/679* (WP 260), texto adoptado el 29 de noviembre de 2017 y revisado el 11 de abril de 2018.

[62] En *http://www.lecturafacil.net/media/resources/2012_CE_Como_escribir_con_claridad.pdf* se pueden consultar las recomendaciones elaboradas por la Comisión Europea para la redacción clara y sencilla de documentos de toda clase (legislación, un informe técnico, actas de reuniones, un comunicado de prensa o un discurso).

[63] El elemento de «fácil acceso» implica un acceso intuitivo y rápido, sin complicaciones para el interesado. Así en *Guidelines on Transparency under Regulation 2016/679* (WP 260), ya citada, punto 11: *«The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc.».*

to, puede ser conveniente arbitrar métodos auditivos o audiovisuales adecuados para los interesados con discapacidad visual, además de cumplir los requisitos de accesibilidad web, con tecnologías de apoyo apropiadas al nivel de discapacidad. Lo mismo, pero a la inversa, cabe señalar para el supuesto —menos frecuente, pero no por ello imposible— de información «verbal» presentada a persona con discapacidad auditiva, a quien, en este caso, deberá poder ofrecérsele la información de forma escrita.

Además, esta obligación de claridad en el lenguaje deberá adaptarse al tipo de público, haciéndose especialmente necesaria cuando los destinatarios son menores de edad[64]; precisamente porque solo se puede autorizar de forma consciente aquello que de verdad se conoce y se entiende.

La información debe ser concreta y categórica; alejada de términos abstractos o ambivalentes que den margen a la interpretación del destinatario. De hecho, sea cual sea la fórmula elegida, la cláusula de consentimiento no podrá mezclarse con otras informaciones, tales como las condiciones de uso o los requisitos del sistema, sino que deberá expresarse de forma separada e individualizada para cada finalidad concreta que se pretenda. Si además el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta dicho consentimiento[65]. Estas consideraciones previas se materializan en el art. 7.2 RGPD:

> «Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de forma tal que se distinga claramente de los demás asuntos».

Y lo que es más importante, a efectos prácticos:

> «No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento».

De modo que aquellas finalidades que se «acomoden» al consentimiento único otorgado de forma genérica para un conjunto de actividades de

---

[64] Considerando 58: «Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender».

[65] Considerando 32 RGPD *in fine*.

tratamiento y que se mezclen con otros mensajes como pueden ser las condiciones de uso, no gozarán de la legitimación requerida y, por tanto, los tratamientos de los datos que se hagan bajo ese «aparente» consentimiento serán ilícitos.

III. LA CARGA DE LA PRUEBA EN LA OBTENCIÓN DEL CONSENTIMIENTO VÁLIDO: LA RESPONSABILIDAD PROACTIVA

Como hemos visto, la nueva normativa condiciona la validez del consentimiento a la concurrencia de los elementos derivados de su definición.

Sin embargo, en el marco del Reglamento, el responsable no solo tendrá que recabar el consentimiento en la forma indicada, sino que, además, deberá haber sido suficientemente precavido a efectos de poder demostrar que el interesado consintió el tratamiento de los datos personales que le conciernen y que dicho consentimiento se otorgó de forma libre, informada, específica y, sobre todo, inequívoca[66]. Y, además, y por si fuera poco, el responsable debe ser capaz de demostrar que es posible retirar el consentimiento recabado de los interesados sin que estos sufran perjuicio alguno. Así lo advierte el considerando 42:

> «Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento [...] El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno».

Ya en el texto del articulado, y con independencia de la licitud del tratamiento[67], el apartado 1 del art. 7 RGPD ratifica la obligación de los responsables de adoptar todas las medidas de responsabilidad activa que

---

[66] Cumple recordar que, en su redacción original, el art. 18.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, preveía la obligación de acreditar el cumplimiento del deber de informar, para lo que exigía la obligación de dejar constancia documental o a través de medios informáticos y telemáticos. El TS anuló el precepto por disconforme a Derecho, al entender que el legislador había optado por la libertad de forma y, en consecuencia, esa conservación excedía de sus previsiones. Así en STS de 15 julio 2010 (RJ 2010\6272), F. 9.º

[67] El deber de transparencia actúa de manera independiente al requisito de los responsables del tratamiento de garantizar que concurre una base jurídica adecuada para el trata-

novedosamente introduce el RGPD en su art. 5.2, recayendo en este caso sobre ellos la carga de la prueba a la hora de tener que demostrar que la persona concernida otorgó su consentimiento:

> «Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales».

Por esto, y dado que el art. 4.11 RGPD no requiere (como regla general) que el consentimiento sea explícito[68], su redacción acepta una multitud de formas válidas para la prestación del consentimiento, que podrá manifestarse ya sea mediante una declaración —verbal o escrita— o mediante una clara acción afirmativa. Lo que viene a suponer la conformidad a todo tipo de fórmulas imaginativas destinadas a obtener el consentimiento, con la sola condición de que resulte verificable *a posteriori*. De tal manera, como ya vimos, la asistencia a un local en el día y en la hora que se han señalado para la celebración de una sesión fotográfica, de la cual se ha informado cumplidamente a cierto público (por ejemplo, a los alumnos de una facultad), define una conducta de la cual se deduce inequívocamente que el interesado acepta el tratamiento de sus datos. La misma conclusión se deriva del comportamiento de quien continúa navegando en una web que utiliza *cookies* y acepta así el que se utilicen *cookies* para monitorizar su navegación. Igual sucede con la solicitud formulada por el responsable a los contactos para que confirmen sus direcciones de correo electrónico antes de ser añadidas a una lista de distribución para recibir comunicaciones vía *email*. El problema tanto en estos casos como en los supuestos de declaración verbal vendrá a la hora de demostrar que el responsable solicitó ese consentimiento previa información y que lo obtuvo convenientemente. Es por eso que, aun dentro de la libertad de forma, el responsable debe idear mecanismos que le permitan guardar testimonio cierto del cumplimiento de sus obligaciones. Para la recogida de datos en sitios web suele resultar determinante la mecánica de funcionamiento del sitio y de sus formularios. De mane-

---

miento con arreglo al art. 6. Así en *Guidelines on Transparency under Regulation 2016/679* (WP 260), nota al pie 14.

[68] Requisito que, como apuntamos, queda limitado a las categorías especiales de datos (art. 9); a las decisiones basadas únicamente en el tratamiento automatizado de datos personales, incluida la elaboración de perfiles [art. 22.1.*c)*], y a la transferencia internacional de datos a terceros países u organizaciones internacionales cuando no haya nivel adecuado de protección (art. 49).

ra que se ha venido admitiendo como prueba del consentimiento la acreditación de que el programa informático impide introducir los datos sin antes haber aceptado la política de privacidad o documento equivalente[69]. Para los consentimientos verbales —por ejemplo, obtenidos por vía telefónica en la oferta de productos de internet o de empresas aseguradoras— la prueba del consentimiento recomendará una grabación de la conversación telefónica.

En todo caso, el responsable habrá de conservar esas pruebas mientras persista su «obligación de poder demostrar», dando fin a este deber al tiempo de concluir la actividad de tratamiento para la que se requirió el consentimiento[70]; momento en que deberá proceder a la eliminación de los datos sin perjuicio de la conservación debida para, en su caso, el cumplimiento de una obligación legal, o por el tiempo que en su caso resulte necesario para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público.

IV. BIBLIOGRAFÍA

Arenas Ramiro, M.: «Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades», en *Hacia un nuevo derecho europeo de protección de datos,* 1.ª ed., Valencia, Tirant lo Blanch, 2015, pp. 311-372.

Arias Pou, M.: «Transparencia e información que deberá facilitarse cuando los datos personales se obtengan del interesado. El derecho a la información desde el diseño (comentario al art. 13 RGPD y al art. 11.1 y 2 LOPDGDD)», en A. Troncoso Reigada (dir.) y J. J. González Rivas (pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos,* vol. I, 1.ª ed., Pamplona, Civitas, 2021, pp. 1357-1379.

Baz Rodríguez, J.: «Protección de datos y garantía de los derechos digitales laborales en el nuevo marco normativo europeo e interno (RGPD 2016 y LOPDPGDD 2018)», *Ars Iuris Salmanticensis (AIS): Revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología,* vol. 7, núm. 1 (2019), pp. 129-171.

---

[69] P. A. de Miguel Asensio, *Derecho Privado de Internet,* 5.ª ed., Cizur Menor, Thomson Reuters, 2015, p. 319, con referencia al Informe AEPD 23/2010.

[70] En pos del principio de «limitación del plazo de conservación» contenido en el art. 5.1.*e)* RGPD.

De Miguel Asensio, P. A.: *Derecho Privado de Internet,* 5.ª ed., Cizur Menor, Thomson Reuters, 2015, p. 319, con referencia al Informe AEPD 23/2010.

Del Castillo Vázquez, I.-C.: *Protección de datos: cuestiones constitucionales y administrativas,* Aranzadi, Cizur Menor, 2007.

Díaz Lafuente, J.: «Transparencia e información al afectado», en M. Arenas Ramiro y A. Ortega Giménez (dirs.), *Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD),* 1.ª ed., Madrid, Sepin Editorial Jurídica, 2019, pp. 91-93.

García Mahamut, R.: «El derecho fundamental a la protección de datos: el Reglamento (UE) núm. 2016/679 como elemento definidor del contenido esencial del art. 18.4 de la Constitución», dispnible en *https://dialnet.unirioja.es/descarga/articulo/6762711.pdf* (consultado el 31 de julio de 2021); trabajo desarrollado por la autora en el marco del proyecto de investigación sobre «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado», Ministerio de Economía y Competitividad (DER 2015-63635-R).

Gonzalo Domenech, J. J., y Bonmatí Sánchez, J.: «Tratamiento basado en el consentimiento del afectado», en M. Arenas Ramiro y A. Ortega Giménez (dirs.), *Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD),* 1.ª ed., Madrid, Sepin Editorial Jurídica, 2019, pp. 69-72.

Martín-Retortillo Baquer, L., y De Otto y Pardo, I.: *Derechos fundamentales y Constitución,* Madrid, Civitas, 1988.

Mayor Gómez, R.: «Principales novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales», *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha,* núm. 16 (2018), pp. 201-246, disponible en *http://gabilex.castillalamancha.es.*

Miralles López, R. M.: «Protección de datos desde el diseño y por defecto (comentario al art. 25 RGPD)», en A. Troncoso Reigada (dir.) y J. J. González Rivas (pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos,* vol. I, 1.ª ed., Pamplona, Civitas, 2021, pp. 1813-1818.

Podlech, A.: «Art. 2, Abs. 1», en *Kommentar zum Grungesetz für die Bundesrepublik Deustchland (Rheine Alternativkommentare),* Neuwied-Darmstadt, Luchterhand, 1984, pp. 41 y ss., citado por A.-E. Pérez Luño, «Los derechos humanos en la sociedad tecnológica», *Cuadernos y Debates,* núm. 21 (1989), pp. 156, nota del autor 20.

Sempere Samaniego, J.: «La licitud del tratamiento», en A. Troncoso Reigada (dir.) y J. J. González Rivas (pr.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos,* vol. I, 1.ª ed., Pamplona, Civitas, 2021, pp. 925-944.

YATES, J.: *Millar v. Taylor,* 4 BURR., 2303, 2379 (1769), citado por S. WARREN y L. BRANDEIS, en B. PENDÁS y P. BASELGA, *El derecho a la intimidad,* 1.ª ed., Madrid, Civitas, 1995, p. 31, nota al pie 16, publicado originalmente en 1890 bajo el título «The Rigth to Privacy», *Harvard Law Review,* vol. IV, núm. 5 (1890).