BASES JURÍDICAS RELEVANTES DEL TRATAMIENTO DE DATOS PERSONALES EN LA CONTRATACIÓN DE CONTENIDOS Y SERVICIOS DIGITALES*

RELEVANT LEGAL BASES IN THE PROCESSING OF PERSONAL DATA IN THE CONTRACTS OF DIGITAL CONTENTS AND DIGITAL SERVICES

Rosa María García Pérez
Profesora Titular de Derecho Civil
Universidad de Granada
ORCID ID: 0000-0002-4817-8102

Recibido: 11.12.2019 / Aceptado: 13.01.2019
DOI: https://doi.org/10.20318/cdt.2020.5228

Resumen: El proceso emprendido a nivel europeo de revisión, modernización y adaptación de las reglas de protección de consumidores al entorno tecnológico ha puesto en contacto dos esferas normativas de contrapuestos intereses: protección de datos personales y Derecho de consumo. El primer punto de inflexión de la compleja interacción entre ambos marcos regulatorios ha venido de la mano de la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos relacionados con los contratos de suministro de contenido digital y servicios digitales, que ofrece los mismos remedios contractuales tanto a consumidores que abonan un precio como a quienes, a modo de contraprestación, facilitan sus datos personales. De las nuevas e interesantes perspectivas de análisis que ofrece la imbricación del derecho fundamental a la protección de datos en la esfera contractual, este trabajo centra su atención en la determinación de las bases de licitud, conforme al Reglamento General de Protección de Datos, de los tratamientos de datos personales derivados del ámbito de aplicación de la Directiva y su incidencia contractual.

Palabras clave: Mercado Único Digital Europeo, interacción derecho de consumo-protección de datos personales, suministro de contenidos y servicios digitales, datos personales como contraprestación, principio de licitud del tratamiento.

Abstract: The European process of revision, modernization and adaptation of consumer protection rules to the technological environment has brought into contact two regulatory spheres of opposite interests: personal data protection and consumer law. The first inflection point of the complex interaction between both regulatory frameworks has come from the hand of Directive (EU) 2019/770 of the European Parliament and of the Council, of 20 May 2019, on certain aspects concerning contracts for the supply of digital content and digital services, which offers the same contractual remedies both to consumers who pay a price and to those who, by way of counter performance, provide their personal data. Of the

*Este trabajo tiene su base en la ponencia expuesta en el Congreso Internacional El Derecho privado en el nuevo paradigma digital (Colegio Notarial de Cataluña, Barcelona, 3 y 4 de octubre de 2019) y se enmarca en el Proyecto I+D (Retos) DER2017-84748-R (Ministerio de Ciencia, Innovación y Universidades): Mercado Único Digital Europeo y Protección de los Consumidores: perfilando los derechos de las partes en contratos de suministro de contenidos digitales, del que es investigador principal el Prof. S. CÁMARA LAPUENTE.

new and interesting perspectives of analysis offered by the overlapping of the fundamental right to data protection in the contractual sphere, this paper focuses on the determination of the bases of lawfulness, according to the General Data Protection Regulation, of the processing of derived personal data of the scope of the Directive and its contractual impact.

Keywords: EU Digital Single Market, interaction consumer law-data protection regulation, supply of digital content and digital services, counter-performance in the form of personal data, principle of lawfulness of the personal data processing.

I. Introducción

1. El acceso *online* a bienes, contenidos y servicios digitales (obras musicales, cinematográficas, literarias, aplicaciones móviles, videojuegos, programas de ordenador, servicios informáticos en la nube, contenidos audiovisuales en *streaming*…) a cambio de datos personales, publicidad, descuentos o ventajas adicionales es hoy día una realidad económica innegable que convive con el tradicional sistema de contratación de base monetaria. Recientes iniciativas y acciones legislativas emprendidas por la Unión Europea en materia de consumidores, tras el lanzamiento de su Estrategia para un Mercado Único Digital en mayo de 2015[1], se han hecho eco, especialmente, del nuevo modelo de negocio basado en transacciones digitales con datos personales que, liderado por grandes empresas tecnológicas, se asienta la mayor parte de las veces en contratos no negociados individualmente, celebrados a menudo por medio de plataformas digitales o *marketplaces*[2]; contratos que, en numerosas ocasiones, el consumidor no percibe como tales[3], sino meramente como un acceso gratuito a bienes, contenidos o servicios digitales. Y con ello los datos personales y su régimen de protección, cuyo principal marco normativo es

[1] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones. *Una Estrategia para el Mercado Único Digital de Europa*. Bruselas, 6.5.2015. COM(2015) 192 final. Accesible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52015DC0192. El último acceso a los sitios web citados en este trabajo se ha realizado con fecha de 12 de diciembre de 2019.

[2] Según estimaciones de Comisión Europea, el 60% del consumo privado y el 30% del consumo público de bienes y servicios se gestionan a través de intermediarios en línea, plataformas y navegadores. Estos intermediarios en línea se benefician y adquieren un gran poder de mercado por los datos que obtienen de la interacción de los usuarios finales con las prestaciones y productos ofertados por los comerciantes. De ahí que la Exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el fomento de la equidad y la transparencia para las empresas que utilizan servicios de intermediación en línea [Bruselas, 26.4.2018 COM(2018). 238 final. 2018/0112 –COD-], los denomine "guardianes de acceso" a los mercados y consumidores, destacando que "la asimetría entre la fuerza relativa de mercado de unas pocas plataformas en línea principales, que no necesariamente se consideran dominantes de acuerdo con el Derecho de la competencia, se ve agravada por la oferta inherentemente fragmentada que conforman miles de pequeños comercios"; Propuesta que ha desembocado actualmente en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019 (DOUE, L 186/57, 11 de julio de 2019).

[3] Sobre la falta de consciencia negocial del usuario de internet y su incidencia en el establecimiento de una auténtica relación contractual, vid. R. Yanguas Gómez, *Contratos de conexión a internet, «hosting» y búsqueda*, Civitas Thomson Reuters, Cizur Menor, 2018, pp. 112-119.

el Reglamento General de Protección de Datos europeo (RGPD) [4], han iniciado una compleja incursión en el Derecho contractual[5].

2. Sin embargo, protección de datos personales y protección de los consumidores en la contratación, aun con objetivos comunes dirigidos al fomento de la transparencia y corrección de asimetrías informativas, son esferas que responden a intereses distintos: naturaleza, régimen jurídico, ámbito de aplicación, remedios, acciones y vías judiciales discurren por caminos diferentes[6]. De hecho la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) y la mayor parte de los textos constitucionales de sus Estados miembros, diferencian claramente, por una parte, el régimen jurídico de protección de los datos personales (artículo 8 CDFUE incardinado en el Título I, dedicado al valor de la "Dignidad") y, por otra, la garantía de un alto nivel de protección de los consumidores (artículo 38 CDFUE inserto en el Título IV bajo la rúbrica "Solidaridad"). Además conviene tener en cuenta que, a diferencia de las normas de Derecho de consumo, el RGPD, como norma general aplicable, cualquiera que sea el contexto en el que se tratan datos personales, incide prácticamente en cualquier sector y, por ende, en el ámbito de las relaciones contractuales.

3. Este alcance general indiscutible ha tomado, no obstante, un nuevo cariz complejo, poliédrico y, en ocasiones, no fácilmente compatible con la concepción y configuración a nivel europeo del derecho fundamental a la protección de datos personales, en el marco de las recientes iniciativas y acciones legislativas emprendidas por la Unión Europea dirigidas a modernizar la normativa de protección de los consumidores.

4. El primer punto de inflexión en este proceso de imbricación del derecho fundamental a la protección de datos en el ámbito contractual ha venido de la mano de la Directiva (UE) 2019/770, de 20 de mayo de 2019, relativa a determinados aspectos relacionados con los contratos de suministro de contenido digital y servicios digitales (DCDig.). Esta Directiva, en la que centraremos nuestra atención en este estudio, sólo es la punta de lanza de una nueva manera de relacionarse normativa de protección de datos personales y normativa de consumo[7].

5. El panorama no quedaría completo sin aludir brevemente a otras medidas enmarcadas en el proceso emprendido a nivel europeo de revisión, modernización y adaptación de las reglas de protección de consumidores al entorno tecnológico, en el marco de la iniciativa "*New Deal for Consumers*", incluida en el Programa de trabajo de la Comisión Europea el pasado 11 de abril de 2018. Se trata de dos propuestas de Directiva[8], una de las cuales ha culminado su tramitación legislativa en fase de confección

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. En trámite se encuentra la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas (Bruselas, 10 enero 2017, COM/2017/010 final), destinado a reemplazar a la vigente Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. No obstante, parece que su aprobación se demorará después del rechazo de la última de sus versiones [Brussels, 15 November 2019 (OR. en) 14054/19] en la reunión negociadora celebrada en el seno del Consejo el pasado 22 de noviembre de 2019.

[5] Compleja interacción que ha llevado a la *41ª Conferencia Internacional de Autoridades de Protección de Datos*, celebrada en octubre 2019, a remarcar la necesidad de estrechar la cooperación en el ámbito digital entre autoridades de protección de datos, de consumo y de defensa de la competencia, vid**.** *Resolution to support and facilitate regulatory co-operation between Data Protection Authorities and Consumer Protection and Competition Authorities to achieve clear and consistently high standards of data protection in the digital economy*, accesible en https://edps.europa.eu/sites/edp/files/publication/dccwg-resolution_adopted_en.pdf.

[6] Así lo expresa M. R. Llácer matacás, *La autorización para el tratamiento de la información personal en la contratación de servicios*, Dykinson, 2012, p. 19: «Son dos planos sometidos a normativa propia, con rango diferente, y sin aparente conexión material: una, la normativa de consumo, persigue la defensa de derechos básicos de corte económico y otra, la tutela de un derecho fundamental».

[7] Interesantes reflexiones sobre la compleja interacción protección de datos-protección de consumidores en N. Helberger, F. Zuiderveen Borgesius & A. Reyna: "In the perfect match? A closer look at the relationship between EU consumer Law and Data protection Law", *Common Market Law Review*, Volume 54, 2017, Issue 5, pp. 1-28. XXXnzadi9 de diciembre de 2015"n i interaccimpartir informaciremitiendo a contactar con el Delegado de Proteccienidos y seevici

[8] Sobre la interferencias de ambas propuestas de Directiva con la normativa de protección de datos se ha pronunciado el Super-

de este trabajo: por una parte, la reciente Directiva 2019/2161/UE destinada a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión[9]; y, por otra parte, la propuesta de Directiva[10] relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores[11].

6. La primera, la Directiva 2019/2161/UE, modifica, entre otras, la Directiva 2011/83/UE, de 25 de octubre de 2011, sobre los derechos de los consumidores. El texto fundamentalmente recoge los siguientes aspectos en lo que aquí interesa:

i. Extensión de su ámbito de aplicación, y en conexión con la DCDig., alcanzará a los contratos de suministro de contenidos o servicios digitales a cambio de que el consumidor proporcione o se comprometa a proporcionar datos personales al comerciante para finalidades diferentes al propio suministro[12].
ii. Ampliación de la transparencia en la contratación a través de intermediarios o proveedores de mercados en línea, definidos como «*aquellos servicios que emplean programas (software) incluidos un sitio web, parte de un sitio web o una aplicación, operados por el comerciante o por cuenta de este, que permite a los consumidores celebrar contratos a distancia con otros comerciantes o consumidores*», imponiéndoles requisitos específicos y adicionales de información precontractual sobre los principales parámetros que determinan la clasificación de las ofertas, sobre si el tercero suministrador es o no un comerciante[13] y si los derechos de los consumidores son o no aplicables.
iii. Además, introduce en la Directiva 2011/83 un nuevo requisito de información[14] al consumidor cuando sus datos personales se traten para elaborar un perfil que permita evaluar su poder adquisitivo y personalizar los precios[15].

---

visor Europeo de Protección de Datos (SEPD) en su *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, 5 de octubre de 2018, accesible en: https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf

[9] Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión (DOUE L328/7, de 18 de diciembre de 2019).

[10] Resolución legislativa [P8-TA-PROV(2019)0222] del Parlamento Europeo, de 26 de marzo de 2019, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores y por la que se deroga la Directiva 2009/22/CE.

[11] Por último, aunque en este caso sin normas sustantivas o procesales en materia de consumo, conviene hacer referencia a la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, cuyo considerando 16 recoge abiertamente un amplio concepto de remuneración, entendiendo que la hay no solo cuando la contraprestación es dineraria, sino también en aquellos casos en que proveedor de un servicio solicita que le sean proporcionados, directa o indirectamente, datos personales u otros datos, como cuando el usuario final facilita el acceso a información sin proporcionarla activamente, como datos personales, entre ellos la dirección IP, u otra información generada automáticamente, como la recopilada y transmitida por una cookie, e incluso se halla expuesto a publicidad para tener acceso al servicio.

[12] Excluyendo, como la DCDig. las situaciones en las que, sin existir contrato, el comerciante sólo recopila metadatos, como información sobre el dispositivo del consumidor o el historial de navegación o el consumidor está expuesto a anuncios exclusivamente para obtener acceso a contenido digital o un servicio digital.

[13] Vid. J. J. Noval Llamas, "El `nuevo marco para los consumidores' y su repercusión sobre el derecho de desistimiento del consumidor. La Comunicación de la Comisión Europea de 11 de abril de 2018 y la propuesta de reforma de la Directiva 2011/83/UE", en P. Castaños Castro y J. A. Castillo Parrilla (Dirs.), *El mercado digital en la Unión Europea*. Ed. Reus. Madrid, 2019, págs. 345-355.

[14] Pero, como advertía S. Cámara Lapuente ("Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad", en P. Castaños Castro y J. A. Castillo Parrilla, *op. cit.*, págs. 242-243) en relación con la Propuesta inicial, en el texto final de la Directiva (UE) 2019/2161, también "se sigue echando en falta un ítem específico de información precontractual sobre los datos (personales y no personales) que se recabarán en contratos sin contraprestación dineraria –pues la referencia al "precio completo" de los arts. 5.1.c) y 6.1.c) de la Directiva 2011/83 no parece cubrir ese extremo– y, más aún, una información previa a la celebración del contrato sobre los derechos de abstención-supresión y recuperación de los contenidos generados por el usuario y otros datos no personales en caso de extinción del contrato".

[15] Vid. R. Tena: "¿Son justos los precios personalizados mediante algoritmos?, *El Notario del siglo XXI*, Nº 87, septiembre-octubre 2019, accesible en http://www.elnotario.es/opinion/9635-son-justos-los-precios-personalizados-mediante-algoritmos.

7. Por otra parte, la Propuesta de Directiva relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, tal y como destaca su considerando 6, incorpora la protección de datos entre los ámbitos cubiertos por la norma y extiende su aplicación tanto a las "infracciones de las disposiciones del Derecho de la Unión que protegen los intereses colectivos de los consumidores, como los intereses colectivos de los interesados en el sentido del Reglamento general de protección de datos*"*[16]. A tal efecto conceptúa como «intereses colectivos de los consumidores»: los intereses de varios consumidores o interesados según el RGPD[17].

8. En este mismo ámbito de defensa de intereses colectivos, la propia DCDig. en su artículo 21.2.d encomienda a los Estados miembros que, entre las medidas articuladas en sus legislaciones nacionales para garantizar el cumplimiento de la norma, prevean el que puedan emprender acciones, ante los órganos jurisdiccionales o ante los organismos administrativos competentes, entre otras, «aquellas entidades, organizaciones o asociaciones sin ánimo de lucro, activas en el ámbito de la protección de los derechos y libertades de los titulares de los datos, tal como se definen en el artículo *80 del Reglamento (UE) 2016/679*»[18].

II. Interacción protección de datos-protección de los consumidores en la Directiva (UE) 2019/770

1. Breves observaciones preliminares sobre el alcance de la norma europea: datos personales a cambio de contenidos y servicios digitales

9. Centrando la atención en la DCDig., conviene comenzar resaltando que esta norma tiene por objeto, tal y como señala su artículo 1, la armonización y el establecimiento de normas comunes sobre ciertos aspectos de los contratos celebrados entre empresarios y consumidores para el suministro de contenidos o servicios digitales[19], en particular, el establecimiento de parámetros para la determinación de

---

Sobre la elaboración de perfiles basada en datos personales, vid. Grupo Trabajo art. 29 (GT29): *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* (adoptadas por última vez el 6 de febrero de 2018).

[16] Tales previsiones, sin duda, incidirán en la aplicación por los Estados miembros del artículo 80 RGPD dedicado a la representación de los interesados; precepto de la norma europea que no ha sido objeto de desarrollo en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales (LOPDGDD).

[17] El RGPD no recoge, sin embargo, la posibilidad de que un determinado particular pudiera entablar una acción colectiva por vulneración de la normativa de protección de datos en nombre de otros que previamente le hayan cedido sus derechos. A tal efecto, conviene hacer mención a la sentencia del Tribunal de Justicia de la Union Europea (TJUE) de 25 de enero de 2018 (*Maximilian Schrems/Facebook Ireland Limited* -asunto C-498/16-) en la que se analiza la posibilidad de que el Sr. Schrems pueda o no acogerse al "fuero del consumidor", que permite a los consumidores de un Estado miembro demandar a una contraparte contractual extranjera ante los tribunales de su domicilio, a fin de que dicho particular pueda entablar una acción colectiva por vulneración de la normativa protectora de datos personales, tras la cesión al mismo de sus específicos derechos por otras personas de diferentes nacionalidades. Vid. P. A. De Miguel Asensio, "Demandas frente a redes sociales por daños en materia de datos personales: precisiones sobre competencia judicial", *La Ley Unión Europea*, Nº 56, 28 de febrero de 2018; L. Moreno García, "Delimitación del «fuero del consumidor» en asuntos relacionados con redes sociales y protección de datos", *Diario La Ley*, Nº 9270, 2 de octubre de 2018; y J. Fernández-Samaniego y B. Piñar Guzmán, "Las acciones colectivas en el marco del RGPD: una perspectiva desde el Derecho Civil español", *Diario La Ley*, Nº 26, Sección Ciberderecho, 11 de febrero de 2019.

[18] En España, la principal campaña de acción colectiva en la que una organización de consumidores está recogiendo mandatos de los interesados es la denominada «*Mis datos son míos*, Mr. *Facebook*», planteada por la Organización de Consumidores y Usuarios (OCU) contra Facebook. En octubre de 2018 presentó una demanda colectiva contra *Facebook,* por cesión irregular de datos, basándose en que la red social no ha informado ni solicitado autorización expresa a los usuarios para la utilización de sus datos. OCU ha ejercitado una acción colectiva en defensa, no solo de los afectados directamente por la filtración de datos Cambridge Analytica, sino de "*todos los usuarios de Facebook en España. En este sentido, la Organización considera que, al haber permitido una gran recopilación e intercambio de datos de sus usuarios sin que estos hayan sido informados ni expresado su conformidad expresa, Facebook ha infringido la Ley de Protección de datos"*. Se solicita resarcir a los usuarios españoles de la red social con la cantidad de, al menos, 200 euros para cada uno. El pasado mes de julio de 2019 fue admitida a trámite por el Juzgado de lo Mercantil número 5 de Madrid. Toda la información está disponible en https://www.ocu.org/especiales/misdatossonmios/.

[19] Tal y como resulta del artículo 4 DCDig. («*Los Estados miembros no podrán mantener o introducir disposiciones contrarias a las establecidas en la presente Directiva, en particular disposiciones más o menos estrictas para garantizar un nivel*

la conformidad de los contenidos o servicios digitales con el contrato, la fijación de medidas correctoras que se atribuyen al consumidor en caso de falta de conformidad o incumplimiento del suministro, y la modificación de los contenidos y servicios digitales. Su alcance se extiende tanto a datos producidos y suministrados por un empresario como a datos generados por los propios consumidores, abarcando los siguientes contratos:

a) contratos de *suministro de "contenido digital",* referidos a datos producidos y suministrados en formato digital (art. 2, n.º 1 DCDig.), incluidos archivos de vídeo, de sonido, aplicaciones, juegos digitales y cualquier otro software. Sería el caso de contenidos obtenidos a través de plataformas de descarga (*Apple Store, Google Play, Amazon*) o de *streaming* (*Apple Music, Amazon Prime Music, Youtube, Vimeo* o *Spotify*);
b) contratos de servicios que permiten *"crear, tratar, almacenar o consultar datos en formato digital".* (art. 2, n.º 2.a DCDig.), como sucede con los servicios *cloud computing* ofrecidos por *Amazon Web Services (AWS), Dropbox, One Drive, Microsoft Azure, Google Cloud, Google Drive, iCloud*; y
c) contratos de "*servicios que permiten compartir datos en formato digital cargados o creados por el consumidor u otros usuarios, o interactuar de cualquier forma con dichos datos.* (art. 2, n.º 2.b DCDig.). Serían los servicios de redes sociales prestados por *Facebook, Twitter, Whatsapp, Instagram, Line, Viber*.

10. En principio, la DCDig. se aplica a aquellos supuestos en los que tales contratos sean celebrados en el ámbito *B2C*, entre empresarios («*toda persona física o jurídica, ya sea privada o pública, que actúe, incluso a través de otra persona que actúe en su nombre o por su cuenta, con un propósito relacionado con su actividad comercial, empresa, oficio o profesión, en relación con los contratos regulados por la presente Directiva*«) y consumidores («*toda persona física que, en relación con los contratos regulados por la presente Directiva, actúa con un propósito ajeno a su actividad comercial, empresa, oficio o profesión*»). No obstante, en sus considerandos, deja una amplia libertad a los Estados miembros para extender su aplicación a «las personas físicas o jurídicas que no sean consumidores…, como organizaciones no gubernamentales, empresas emergentes y pymes» (considerando 16) o a calificar como consumidores a quienes celebran «contratos con doble objeto», en parte relacionado y en parte no con la actividad comercial de la persona, o «en los que el objeto comercial es tan limitado que no predomina en el contexto general del contrato» (considerando 17).

11. Asimismo contempla el fenómeno de la contratación mediante plataformas en línea. En este sentido, al delimitar el concepto de empresario, el considerando 18 DCDig. advierte: «Los prestadores de plataformas pueden ser considerados empresarios a los efectos de la presente Directiva si actúan con fines relacionados con sus propias actividades y en calidad de socio contractual directo del consumidor en el suministro de contenidos o servicios digitales»[20]. Y deja libertad a los Estados miembros para «ampliar la aplicación de la presente Directiva a los prestadores de plataformas que no cumplan los requisitos para ser considerados empresarios a los efectos de la presente Directiva»[21].

diferente de protección de los consumidores»), se trata de una armonización plena, con la finalidad de eliminar la disparidad legislativa actualmente existente y garantizar un elevado nivel de protección de los consumidores, contribuyendo al establecimiento de un marco jurídico que beneficie el buen funcionamiento del mercado interior.

[20] La expresión "socio contractual directo del consumidor", de difícil intelección en nuestro sistema, es transcripción literal de la versión inglesa de la DCDig.; debe ser entendida como como "parte contractual directa del consumidor", de modo que la norma será aplicable a aquellos supuestos en los que la plataforma se presenta e identifica como proveedora directa del contenido o servicio digital, no resultando aplicable, en principio, a los operadores de plataformas que son utilizadas por los proveedores para exhibir y suministrar sus productos, esto es, a los intermediarios o proveedores de mercados en línea (por ejemplo, plataformas o portales en línea pertenecientes a un tercero distinto del suministrador). En estos casos, la operación subyacente no sería calificada como suministro directo del operador de la plataforma-empresario al consumidor.

[21] A efectos de cumplimiento de la obligación de suministro conforme al artículo 5 DCDig., el considerando 41 aclara la responsabilidad del empresario que utiliza plataformas de intermediación *online* para facilitar al consumidor el acceso o puesta a disposición de las prestaciones digitales: «Debe considerarse que los contenidos o servicios digitales están disponibles o accesibles para el consumidor cuando los contenidos o servicios digitales, o cualquier medio adecuado para acceder a ellos o descargarlos,

12. Ahora bien, sin perjuicio de la transposición que se realice de la Directiva, a efectos de determinar si el operador de la plataforma es un mero intermediario (siéndole de aplicación el régimen de prestadores de servicios de la sociedad de la información de conformidad con la Directiva 2000/31 sobre servicios de la sociedad de la información[22]) o puede ser considerado el prestador mismo del servicio subyacente (y, en consecuencia, obligado a garantizar la conformidad de los contenidos y servicios digitales con el contrato y a responder en los términos previstos en la DCDig.[23]), conviene tener presentes los criterios diseñados por el TJUE en sentencia 2017/217, de 20 de diciembre de 2017 (C-434/15, *Asociación Profesional Taxi Élite vs Uber Systems Spain, S.L.*) y los señalados por la Comisión Europea en la *Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una Agenda para la Economía colaborativa* de 2 de junio de 2016[24]. Para el TJUE y la Comisión Europea, el criterio conforme al cual el operador de la plataforma, además de intermediario, puede ser considerado proveedor de servicio subyacente es que tenga una influencia decisiva en la organización y condiciones de las prestaciones efectuadas por el proveedor, lo cual debe valorarse caso por caso. Además, tal influencia decisiva no concurrirá cuando la actividad de las plataformas no sea transaccional, limitándose a ofrecer publicidad o enlaces webs a proveedores; ofrezca herramientas técnicas para facilitar el encuentro entre oferentes, profesionales o no, y demandantes; recomiende (pero no imponga) tarifas; prevea mecanismos de evaluación o calificación de proveedores; u ofrezca algún servicio accesorio como la gestión del pago, un seguro de cobertura o un servicio post venta. Asimismo, es de interés a estos efectos, la propuesta académica de Directiva de plataformas en línea elaborada por el *Research Group on the Law of Digital Services*[25].

13. Pero, sin duda, uno de los aspectos más novedosos de la norma europea viene de la mano de su aplicación, tanto a aquellos contratos en que el empresario suministra contenidos o servicios digitales al consumidor y este paga o se compromete a pagar un precio, como cuando el consumidor «*facilite o se comprometa a facilitar datos personales al empresario, salvo cuando los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales con arreglo a la presente Directiva o para permitir que el empresario cumpla los requisitos legales a los que está sujeto, y el empresario no trate esos datos para ningún otro fin*» (artículo 3.1. párrafo segundo DCDig.). Tales datos personales facilitados con finalidades distintas al sumnistro

hayan llegado al entorno del consumidor y no sea necesario ningún otro acto del empresario para que el consumidor pueda utilizarlos conforme al contrato. Habida cuenta de que el empresario no es en principio responsable de los actos u omisiones de un tercero que gestione una instalación física o virtual, por ejemplo, una plataforma electrónica o una instalación de almacenamiento en nube, que el consumidor elija para recibir o almacenar los contenidos o servicios digitales, debe ser suficiente que el empresario suministre los contenidos o servicios digitales a dicho tercero. No obstante, no puede considerarse que el consumidor haya elegido la instalación física o virtual si está sometida al control del empresario o vinculada contractualmente a él, o cuando el consumidor haya seleccionado dicha instalación física o virtual para recibir los contenidos o servicios digitales pero esa opción era la única ofrecida por el empresario para recibir o acceder al contenido digital o al servicio digital. […] En esos casos, el consumidor debe contar con las mismas medidas correctoras que si el empresario no hubiera suministrado el contenido digital o el servicio digital».

[22] Y la consiguiente exención de responsabilidad por la ilicitud de los datos alojados en la plataforma, como falsedad de ofertas de proveedores o evaluaciones de los usuarios, salvo que tenga conocimiento efectivo y no actúe diligentemente para eliminarlos o no se limite a realizar un tratamiento meramente neutro, pasivo y automátivo de los datos.

[23] Recientemente, sobre la contratación mediante plataformas y su régimen de responsabilidad, vid. F. Pertíñez Vílchez, "La responsabilidad de la plataforma como prestador del servicio subyacente", en A. Orti Vallejo y G. Rubio Gimeno (Dirs.), *Propuestas de regulación de las plataformas de economía colaborativa: perspectivas general y sectoriales*, Thomson Reuters Aranzadi, Cizur Menor, 2019, pp. 141-155 y "La economía colaborativa en la estrategia del Mercado Digital Único de la Unión Europea", en P. Castaños Castro y J. A. Castillo Parrilla *El mercado digital en la Unión Europea, cit.* pp. 152 y ss.

[24] Bruselas, 2.6.2016 COM(2016) 356 final.

[25] Research Group on the Law of Digital Services**:** *Discussion Draft of a Directive on Online Intermediary Platforms*, *Journal of European Consumer and Market Law, EuCML*, Volume 5, Issue 4/2016, pp. 164-169. El artículo 18 de la Propuesta académica prevé la responsabilidad del operador de la plataforma por incumplimiento de proveedores en aquellos casos en que el cliente pueda confiar razonablemente en que el operador de la plataforma tiene una influencia predominante sobre el proveedor, estableciendo como criterios para evaluar este extremo los siguientes: a. El contrato se celebre exclusivamente a través de herramientas provistas por la plataforma; b. El operador de la plataforma retenga los pagos realizados por clientes; c. Los términos del contrato sean esencialmente determinados por el operador de la plataforma; d. El precio a pagar por el cliente esté determinado por operador de plataforma; e. El operador de la plataforma proporcione una marca comercial o imagen uniforme de los proveedores; f. El marketing o estrategia publicitaria sea fijada por el operador de la plataforma y no por los proveedores; g. El operador de la plataforma monitoree la conducta de proveedores.

pueden ser proporcionados por el consumidor, bien en el momento en que se celebre el contrato, bien en un momento posterior: «la presente Directiva debe aplicarse en aquellos casos en que el consumidor abre una cuenta en una red social y facilita un nombre y una dirección de correo electrónico, y estos se utilizan para fines que no sean exclusivamente el suministro de los contenidos o servicios digitales, o distintos del cumplimiento de los requisitos legales. También debe aplicarse en aquellos casos en que el consumidor dé su consentimiento para que cualquier material que constituya datos personales, como fotografías o mensajes que cargue, sea tratado por el empresario con fines comerciales» (considerando 24 DCDig.).

14. Esta suerte de equiparación entre contraprestación dineraria y contraprestación no dineraria en forma de datos personales, que hunde sus raíces en la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una normativa común de compraventa europea de 2011[26] y fue tomada en consideración por la Comisión Europea al interpretar la Directiva 2011/83/UE para incoporarlos en su ámbito de protección[27], ha sido uno de los aspectos más controvertidos en la tramitación legislativa de la Directiva[28].

Inicialmente, la Propuesta DCDig. presentada por la Comisión, aludía a contratos sobre contenidos digitales a cambio del pago de un precio o en los que «el consumidor facilita activamente otra contraprestación no dineraria en forma de datos personales o de otro tipo de datos» (art. 3.1). La vehemente reacción del Supervisor Europeo de Protección de Datos (SEPD) a la mercantilización de los datos personales[29], propia del ámbito anglosajón ("*data as commodity*")[30], derivada de la propuesta

[26] Comisión Europea: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una normativa común de compraventa europea, Bruselas, 11 octubre 2011 COM(2011) 635 final 2011/0284 (COD). En su considerando 18 se reconocía: «A menudo, los contenidos digitales no se suministran a cambio de un precio sino en combinación con bienes o servicios pagados por separado, lo que implica consideraciones no pecuniarias como, por ejemplo, el acceso a datos personales o el acceso gratuito en el contexto de una estrategia de marketing basada en la expectativa de que el consumidor adquirirá posteriormente contenidos digitales adicionales o más sofisticados. Habida cuenta de esta estructura de mercado específica y del hecho de que los defectos de los contenidos digitales suministrados pueden ir en contra de los intereses económicos de los consumidores, independientemente de las condiciones en las que se suministraron, la aplicabilidad de la normativa común de compraventa europea no debe depender de si se paga un precio o no por el contenido digital en cuestión». De ahí que su artículo 5 estableciera que se podrá recurrir a la normativa común de compraventa europea para regular: «b) los contratos de suministro de contenidos digitales, independientemente de que se suministren o no en un soporte material, que puedan ser almacenados, tratados y reutilizados por el usuario, o a los que este pueda tener acceso, tanto si los contenidos digitales se suministran a cambio del pago de un precio como si no».

[27] Vid. Comisión Europea. DJ Justicia: *Documento de orientación relativo a la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo*, 20 junio 2014, p. 72, epígrafe 12.1: «de acuerdo con la distinción realizada en el considerando 19, los contratos para contenidos digitales en línea están sujetos a la Directiva si no implican el pago de un precio por parte del consumidor. De hecho, si bien la Directiva, en su artículo 2, apartados 5 y 6, define «contrato de venta» y «contrato de servicios» como contratos en los que el consumidor paga o se compromete a pagar un precio, la Directiva no contempla ninguna disposición por la que los contratos para contenidos digitales en línea estén sujetos a un requisito similar de que el consumidor tenga que pagar un precio. Incluir contratos para contenidos digitales en línea gratuitos amplía considerablemente el ámbito de aplicación de la Directiva. »

[28] Vid. L. Drechsler, "*Data As Counter-Performance: A New Way Forward or a Step Back for the Fundamental Right of Data Protection?*", *Jusletter IT* 22, febrero 2018, accesible en SSRN (https://ssrn.com/abstract=3329345); A. Metzger, *"Data as Counter-Performance. What Rights and Duties do Parties Have?"*, *JIPITEC* 8 (1), 2017, pp. 2-3; A. Metzger, Z. Efroni, L. Mischau y J. Metzger, "*Data-Related Aspects of the Digital Content Directive", JIPITEC*, 9, 2018, pp. 93-96; y R. Sánchez Lería, "El contrato de suministro de contenidos digitales a cambio de datos personales: a propósito de la propuesta de directiva 634/2015 de 9 de diciembre de 2015", *Revista Aranzadi de Derecho Patrimonial*, Nº 45, 2018.

[29] Vid. SEPD: *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content,* 14 de marzo de 2017 (accesible en https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf). El SEPD llega a comparar el intercambio de datos personales con el tráfico de órganos humanos: «*There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation*» (apartado 17, p. 7).

[30] En EEUU, la reciente "California Consumer Privacy Act of 2018", aprobada el pasado 28 de junio de 2018 y en vigor a partir de 2020, recoge un amplio catálogo de derechos de los consumidores en relación con la protección de sus datos, incluyendo la facultad de venderlos a cambio de un precio. La ley reconoce también a las empresas la posibilidad de ofrecer a los consumidores ciertos incentivos financieros por la recopilación, venta y eliminación de su información personal. Estos incentivos pueden variar en función del valor aportado al comprador por los datos del consumidor. Pero el punto de partida de la norma americana es completamente distinto al europeo: es legítimo por parte de las empresas obtener beneficios del tratamiento de la información personal, salvo que el consumidor se oponga ejerciendo su derecho de exclusión (*op out*).

normativa no se hizo esperar. En su dictamen rechazó «cualquier nueva disposición que introduzca la idea de que los ciudadanos pueden pagar con sus datos del mismo modo que con su dinero. [Los] Derechos fundamentales […] no pueden quedar sometidos al puro interés de los consumidores, como tampoco deben considerarse los datos personales como una mera mercancía». Asimismo manifestó su discrepancia con varios aspectos concretos: la no definición de lo que sea "contraprestación" ("*counter-performance*") cuando existen usos distintos de los datos a la estricta "prestación" del servicio (mejorar la calidad de éste o personalizarlo, por ejemplo); la facilitación "activa" de los datos no solo se considera una acotación insostenible (también a la luz del RGPD) sino engañosa, pues los consumidores muchas veces no son conscientes de que los facilitan ni para qué exactamente; la imposible equivalencia entre dinero y datos, pues dar los últimos no priva al titular de darlos a otra persona ni es posible determinar el valor generado con sus datos, a efectos de la obligación de restitución. Por todo ello, el SEPD ofrece dos alternativas para abordar la cuestión en la Propuesta DCDig.: bien usar la noción de "servicios" en los que, según la normativa europea (vid. la Directiva de comercio electrónico), no es de esencia el pago de remuneración, o bien tomar como modelo la fórmula de describir el ámbito territorial del RGPD (art. 3.2.a), que cubre, sin hablar de "contraprestación", «la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago».

En su paso por el Parlamento Europeo, la Propuesta se remitió a la Comisión de Mercado Interior y Protección del Consumidor y a la Comisión de Asuntos Jurídicos, en cuyo informe conjunto se proponía eliminar el término "contraprestación", criticado por el SEPD, y reemplazarlo por "condición": la Directiva sería aplicable a los contratos en los que el consumidor paga un precio y a los contratos en los que el contenido o servicio digital se suministra bajo la condición de que "*el consumidor facilite datos personales o sean recogidos por el comerciante o una tercera parte en interés del comerciante*", excluyendo de su ámbito, no sólo aquellos supuestos en que los datos facilitados por el consumidor o recogidos por el comerciante sean procesados exclusivamente para suministro, sino tambien cuando se limite a tratarlos para *"mantener la conformidad o mejorar sus contenidos o servicios digitales*"[31]. En los últimos pasos de la tramitación legislativa se elude el término contraprestación: el art. 3.1 Propuesta DCDig.-Parlamento señalaba que la Directiva no se aplicará cuando el consumidor no pague un precio «ni proporcione o se comprometa a proporcionar datos personales al proveedor"; por su parte, el art. 3.1 Propuesta DCDig.-Consejo, se pronunciaba en positivo, siendo aplicable la norma si el empresario suministra contenidos o servicios digitales al consumidor «mediante el pago de un precio o con la condición de que el consumidor facilite datos personales o que sean recogidos por el comerciante».

El 1 de junio de 2017, el Consejo adoptó una Orientación general que, siguiendo la línea del SEPD, elimina el término "contraprestación" y propone incluir en el ámbito de aplicación de la Directiva «a cualquier contrato en el que el proveedor suministre o se comprometa a suministrar contenido digital o un servicio digital al consumidor», y excluir tanto el «suministro de contenidos o servicios digitales por los que el consumidor no pague o se comprometa a pagar un precio ni proporcione o se comprometa a proporcionar datos personales al proveedor», añadiendo que «tampoco se aplicará cuando el proveedor trate los datos personales exclusivamente para suministrar el contenido o servicio digital, o para que el proveedor cumpla los requisitos legales a los que está sometido, y cuando el proveedor no trate los datos de otra manera".

En la fase de trílogos, el 29 de enero de 2019, se adoptó un acuerdo provisional del que, entre otras cuestiones, resultó la redacción finalmente contenida en la DCDig. y aprobada por el Parlamento en primera lectura el 1 de abril de 2019.

15. Las previsiones del artículo 3 DCDig. relativas a los contratos incluidos en su ámbito de protección deben completarse con algunas aclaraciones contenidas en sus considerandos. Así, la aplicación de la DCDig. queda excluida no sólo cuando, sin contraprestación dineraria, los datos facilitados al empresario son tratados por este exclusivamente con el fin de suministrar contenidos o servicios digitales o para que este cumpla requisitos legales (artículo 3.1), sino también cuando, sin haberse concluido un contrato, el suministrador únicamente recoge metadatos tales como información sobre el dispositivo del

[31] Parlamento europeo. Comisión de Mercado Interior y Protección del Consumidor - Comisión de Asuntos Jurídicos (A8-0375/2017): *Informe sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales*. Noviembre, 2016. Enmiendas 80 y 83, pp. 56-58.

consumidor o el historial de navegación o el consumidor se expone a recibir publicidad con el fin exclusivo de obtener acceso a contenidos o servicios digitales (considerando 25). En tales supuestos, tan frecuentes en la navegación por intenet en los que se utilizan dispositivos o técnicas de almacenamiento y recuperación de datos (como *cookie*s, *local shared objects* o *flash cookies* , *web beacons* o *bugs*, tecnologías *fingerprintin*g, etc. [32]) que inciden en la privacidad de las personas y pueden conllevar el tratamiento de datos personales[33], lo decisivo, a efectos de aplicación de la norma, será determinar si se ha celebrado o no un contrato con arreglo al Derecho nacional[34]. No obstante, una vez más, la DCDig. deja libertad a los Estados miembros para ampliar su ámbito de aplicación a tales situaciones excluidas[35].

2. La imbricación del derecho fundamental a la protección de datos en el ámbito contractual delimitado por la Directiva

16. Con la toma en consideración de las transacciones de prestaciones digitales a cambio de datos personales en la DCDig., la Unión Europea ha iniciado un camino de interconexión entre la normativa de protección de datos y el derecho de consumo, que algún autor ha dado en llamar "*contractualiza-*

[32] Sobre estas técnicas y su incidencia en la privacidad pueden consultarse dos recientes documentos de la Agencia Española de Protección de Datos (AEPD): *Estudio fingerprinting o huella digital del dispositivo*, febrero 2019 (accesible en https://www.aepd.es/media/estudios/estudio-fingerprinting-huella-digital.pdf) y *Guía sobre el uso de las cookies*, noviembre 2019 (accesible en https://www.aepd.es/media/guias/guia-cookies.pdf). Además de las *cookies* tradicionales (líneas de texto creadas en el navegador del usuario para registrar su actividad), existen otras técnicas de rastreo a las que se alude en los documentos mencionados:

– *Local shared objects* o *flash cookies*: son un tipo de *cookie*s que pueden almacenar mucha más información que las *cookies* tradicionales. Al ser independientes del navegador utilizado son más difíciles de localizar, visualizar o borrar y pueden utilizarse, por ejemplo, para regenerar cookies estándar.

– *Web beacons* o *bugs*: son imágenes, inapreciables a la vista por su tamaño y color, que se descargan al visitar una web pero que están almacenadas en un segundo sitio y que permiten al titular de ese segundo sitio registrar la visita mediante la información que el navegador de éste proporciona al descargar la imagen (dirección IP, sistema operativo, versión de navegador, etc.).

– *Fingerprinting* o huella digital del dispositivo, es un conjunto de datos extraídos del terminal del usuario que permiten individualizar de forma unívoca dicho terminal. Dado que lo habitual es que las personas no compartan sus equipos, ya sea este un teléfono móvil, tableta, portátil u ordenador de trabajo, individualizar el terminal supone individualizar a la persona que lo utiliza.

[33] La Autoridad de Control francesa (CNIL) ha puesto a disposición de los usuarios en su web una herramienta (*cookieviz*) para escanear *on line* los rastreadores almacenados en los dispositivos de los usuarios por prestadores de servicios de la sociedad de la información. Puede accederse a ella en https://linc.cnil.fr/fr/cookieviz-une-dataviz-en-temps-reel-du-tracking-de-votre-navigation

[34] Este aspecto (existencia o no de contrato conforme a la legislación nacional) introduce un matiz diferencial respecto de la propuesta inicial de Directiva de la Comisión Europa [Bruselas, 9.12.2015 COM(2015) 634 final 2015/0287 (COD)] que abiertamente excluía del ámbito de aplicación, en su considerando 14, las situaciones en las que el proveedor recaba información, incluidos datos personales, tales como la dirección IP u otra información generada automáticamente como información recogida y transmitida por una *cookie*, aunque el consumidor la acepte, así como aquellas en las que el consumidor se expone a recibir publicidad con el fin exclusivo de obtener acceso a contenidos digitales. Tales exclusiones, así como la exigencia de que el consumidor facilitase activamente los datos, fueron duramente criticados por la doctrina por la amplitud de contratos que quedaban al margen del régimen de protección de la Directiva, vid., además de autores citados en nota 28, H. Beale: "Scope of application and general approach of the new rules for contracts in the digital environment", en *Workshop for the (JURI) Committee on Legal Affairs, European Parliament: New rules for contracts in the digital environment, with the participation of EU National Parliaments*, Brussels, 17 febrero 2016, pp. 12-14, accesible en http://www.europarl.europa.eu/cmsdata/98770/Beale.pdf; S. Cámara Lapuente: "El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015", *Indret: Revista para el Análisis del Derecho*, N.º 3, julio 2016, pp. 22-26 y "Una prospectiva crítica sobre el régimen de los contratos de suministro de contenidos digitales", en F. Capilla Roncero, M. Espejo Lerdo de Tejada, F. J. Aranguren Urriza, J. P. Murga Fernández (Dirs.), *Derecho digital: retos y cuestiones actuales*, Aranzadi Thomson Reuters, Cizur Menor, 2018, pp. 52-55; M. B. M. Loos: "*Not good but certainly content: the Proposals for European Harmonisation of Online and Distance Selling of Goods and the Supply of Digital Content*", en *Digital content & distance sales : new developments at EU level*, eds**.** I. Claeys, E. Terryn. Intersentia, 2017, p. 29.

[35] Para una crítica sobre la falta de armonización que implica dejar a las legislaciones nacionales la caracterización o no como contratos de estas situaciones, vid. R. Robert y L. Smit: "*The proposal for a directive on digital content: a complex relationship with data protection law*", *ERA Forum* (2018) 19, pp. 172 (159-177). DOI 10.1007/s12027-018-0506-7. Consciente de ello, el legislador europeo prevee una revisión de la aplicación de la Directiva, a más tardar, el 12 de junio de 2024, mediante un informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo que «*examinará, entre otras cuestiones, el supuesto de armonización de las normas aplicables a los contratos de suministro de contenidos o servicios digitales distintos a los previstos en esta Directiva, incluidos los suministrados a cambio de anuncios publicitarios*» (art. 25 DCDig.).

ción del derecho fundamental a la protección de datos personales"[36]; interconexión relevante desde una doble perspectiva. En primer lugar, por la vía de reconocer la existencia de reciprocidad u onerosidad[37] en aquellos contratos en los que el consumidor permite el tratamiento de sus datos personales a cambio de acceder a prestaciones digitales, otorgándole la misma protección que si su contraprestación hubiese sido dineraria[38]. Este es el objetivo perseguido por el legislador europeo: «garantizar que los consumidores, en el contexto de dichos modelos de negocio, tengan derecho a medidas correctoras contractuales» (considerando 24 DCDig.). En segundo lugar, por la incidencia que la normativa de protección de datos y, en particular, su contravención, puede tener como criterio de validez y eficacia contractual.

17. Esta doble vía de interacción RGPD-DCDig. suscita algunos aspectos conflictivos en los que se pone de manifiesto la tensión entre dos enfoques regulatorios contrapuestos; tensión que ha estado presente a lo largo de toda la tramitación legislativa, saldada en el texto final de la DCDig. con una mención expresa a la prioridad de aplicación del RGPD en caso de colisión: «*El Derecho de la Unión en materia de protección de datos personales se aplicará a cualesquiera datos personales tratados en relación con los contratos contemplados en el apartado 1. En particular, la presente Directiva se entenderá sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. En caso de conflicto entre las disposiciones de la presente Directiva y el Derecho de la Unión en materia de protección de datos personales, prevalecerá el segundo*» (art. 3.8 DCDig.). Queda pues patente que la relación DCDig.-RGPD no es la existente entre una norma general que deba ceder en su aplicación ante la existencia de una específica como sucede cuando la propia DCDig. declara su subsidiariedad respecto de otras normas de la Unión Europea que regulen un sectores específicos (art. 3.7 DCDig.).

18. No obstante esta prioridad, hay aspectos de la Directiva que, puestos en contacto con el régimen normativo de protección de datos, siguen siendo fuente de fricción. Así en el momento del inicio de la relación contractual, surge la cuestión relativa a la concreción de la base jurídica que, conforme a las previsiones del artículo 6 RGPD, da soporte a los tratamientos derivados de contratos a los que resulta aplicable la DCDig. (¿consentimiento ex art. 6.1.a RGPD?; ¿ejecución de un contrato ex art. 6.1.b. RGPD?; ¿interés legítimo ex art. 6.1.f RGPD?); en la fase de ejecución del contrato, cabe plantear si los principios y obligaciones impuestos por el RGPD al responsable del tratamiento de datos-proveedor tienen o no alguna repercusión en la evaluación de la conformidad con el contrato de los contenidos y servicios digitales; y, finalmente, llegado el momento de finalización del contrato, es de interés analizar qué efectos tiene la extinción contractual en el tratamiento de datos personales y en los derechos que ostenta el consumidor-interesado conforme al RGPD y la LOPDGDD.

---

[36] Así, A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*. Edizioni Scientifiche Italiane, Nápoles 2017, pág. 9.

[37] Sobre el carácter oneroso de estos contratos, vid. F. M. Roselló, "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales". *Revista de Derecho Mercantil*. N.º 303, 2017, pp. 163-190.

[38] Sirvan como contraste de esta concepción las palabras de M. R. Llácer matacás (*op. cit*., pp. 105-106): «Las "contraprestaciones" en forma de descuentos, regalos o participación en sorteos no son indicativas de un contrato ya que los datos no pueden constituir su objeto (art. 1254 CC). Se descarta pues la causa onerosa en su sentido objetivo de interdependencia entre las prestaciones derivadas del tipo contractual (cfr. art. 1274 CC). Tampoco se aprecia una onerosidad mediata como la reconocida en el Anexo a) de la Ley 34/2002, de 11 julio, de servicios de la sociedad de la información y de comercio electrónico que, al definir los "servicios de la sociedad de la información", comprende "los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios". El negocio unilateral de autorización es abstracto. En este sentido la autorización puede hacerse en contemplación de una contraprestación positiva (obtención de ventajas o servicios) o negativa (rebaja o gratuidad, como en el mencionado caso Gratis Tel). A diferencia de la onerosidad impropia o derivada del tipo contractual, nos hallamos ante un intercambio desprovisto de volición conjunta que, eventualmente, coexiste con un contrato que sirve de mecanismo para hacer llegar al consumidor la solicitud de autorización. Se trata de una onerosidad económica, extrínseca al negocio, y que explica que la autorización tanto pueda hacerse "por precio" como sin contrapartida […]. En definitiva, creemos que la onerosidad no representa un problema jurídico: no lo hay en cuanto a su admisibilidad, dada la mencionada abstracción de la autorización, ni produce confusión sobre la naturaleza jurídica de la autorización. En cambio, sí que plantea una cuestión de política legislativa y justifica acciones para fortalecer el régimen de protección de los individuos frente a la captación profesional de datos personales, predispuesta por los interesados en obtenerlos y más atractiva cuando se vincula a una "contraprestación"».

19. El primero de los aspectos reseñados, único al que se dedicará este trabajo, la fijación de base legal del tratamiento de datos personales, particularmente de aquellos datos facilitados para ser tratados por el proveedor con finalidades distintas al suministro de contenidos o servicios digitales o al cumplimiento de requisitos legales, no es una cuestión baladí, ni desde la óptica de la normativa de protección de datos (*ad. ex.*, contenido obligatorio del deber de información *ex* artículos 13.1c, 14.1.c y 14.2.b RGPD, amplitud de los derechos de los interesados establecidos en los artículos 15 a 22 RGPD…), ni desde la perspectiva de las repercusiones que sobre el propio contrato de suministro puedan tener la opción por una u otras bases (v.gr., si la licitud del tratamiento es el consentimiento del titular de los datos ¿su revocación lleva aparejada la resolución contractual?; ¿supondría dejar la validez y cumplimiento del contrato al arbitrio de una de las partes?...).

20. El segundo, cuyo análisis se pospone para un ulterior trabajo, atinente al cumplimiento por el proveedor de los principios que, conforme al artículo 5 RGPD, deben ser observados en cualquier tratamiento de datos personales, implica responder a la siguiente cuestión: ¿un tratamiento de datos realizado por el suministrador que infrinja alguno de los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización, etc., puede determinar, al margen de los mecanismos de reacción propios del derecho fundamental a la protección de datos, una falta de conformidad activadora de las medidas correctoras establecidas por la DCDig.?

21. La intersección protección de datos-suministro de contenidos digitales en el momento de la extinción contractual plantea el interrogante acerca de cuál sea el destino de los contenidos, datos personales y no personales, sobre los que tenía control el consumidor durante la relación contractual y la puesta en contacto de sus derechos a la recuperación de contenidos y abstención de su utilización por el proveedor previstos en la DCDig. con los derechos de portabilidad, supresión y olvido respecto de contenidos que sean datos personales conforme al RGPD y la LOPDGDD; materia que aborda ampliamente en este número de la Revista el profesor CÁMARA LAPUENTE[39].

III. El principio de licitud del tratamiento y su incidencia en los contratos amparados por la Directiva

22. Asumido que los contratos a los que extiende su protección la DCDig. comportan el tratamiento de datos personales, el considerando 38 de la norma deja claro que su misión no es interferir en las condiciones para el tratamiento lícito de tales datos, por cuanto esta cuestión está regulada por el RGPD[40]. Por consiguiente, cualquier tratamiento de datos personales en relación con un contrato que tenga encuadre en su ámbito de aplicación solo será **lícito** si concurre una base o causa de legitimación de las previstas legalmente en el artículo 6.1 RGPD, a saber:

a) el consentimiento prestado por el interesado para el tratamiento de sus datos para uno o varios fines especificos;
b) la necesidad del tratamiento para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) la necesidad del tratamiento para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) la necesidad del tratamiento para proteger intereses vitales del interesado o de otra persona física;

[39] Y, anteriormente, en "Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos…", *cit.*, pp. 157-249.

[40] Considerando 38 DCDig.: «La presente Directiva no debe regular las condiciones para el tratamiento lícito de datos personales, por cuanto esta cuestión está regulada, en particular, por el Reglamento (UE) 2016/679. Por consiguiente, todo tratamiento de datos personales en relación con un contrato que entre en el ámbito de aplicación de la presente Directiva solo es lícito si es conforme a lo dispuesto en el Reglamento (UE) 2016/679 en relación con los fundamentos jurídicos para el tratamiento de los datos personales».

e) la necesidad del tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) la necesidad del tratamiento 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.

23. Pues bien, dentro de este catálogo de posibles bases jurídicas que legitiman el tratamiento de datos personales cabe plantearse: ¿cuál es la que da soporte a los tratamientos derivados de los contratos a los que resulta aplicable la DCDig.? La concreción de la base legal del tratamiento no es una cuestión menor, ni desde la perspectiva de la normativa de protección de datos ni desde la vertiente de las repercusiones que sobre el propio contrato de suministro puedan tener una u otra.

24. Desde la óptica de protección de datos, la base de legitimación está directamente relacionada con los principios de legalidad, lealtad y limitación de la finalidad. El responsable de tratamiento de datos personales debe de ser preciso y riguroso en esta materia, determinando la base legal antes de comenzar la actividad de tratamiento en relación con fin específico para que se recogen los datos, dado que tales bases no son intercambiables (por ejemplo, el responsable no puede pasar del consentimiento a otras bases jurídicas constante el tratamiento) y se incorporan al contenido obligatorio del deber de información (artículos 13.1c, 14.1.c y 14.2.b RGPD) que debe facilitarse al interesado en el momento en que se obtengan los datos personales; además, en aplicación del principio de responsabilidad proactiva (arts. 5.2 y 24 RGPD), deberá poder demostrar la adecuación de la base jurídica utilizada a las exigencias del RGPD (así, si el tratamiento de datos va a tener lugar porque concurra una causa de legitimación distinta al consentimiento, pero este se requiere del interesado, tal solicitud puede inducir a error al titular de los datos al creer que ostenta el control)[41]; por último, la opción por una u otra base de licitud puede repercutir en los derechos atribuidos al titular de los datos frente a ese tratamiento, determinando una mayor o menor amplitud. Así, por ejemplo:

a. Cuando la base legitimadora es el consentimiento o la ejecución de un contrato, entran en juego el derecho de portabilidad y el derecho al olvido, pero no el de oposición ni el específico de oponerse a decisiones basadas en el tratamiento automatizado de datos, incluida la elaboración de perfiles, dado que se permiten tales decisiones cuando son necesarias para la celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento, o si se consienten explícitamente. Aunque cuando el tratamiento tiene base en el consentimiento, su revocación opera de manera más amplia que el derecho de oposición en el caso del interés legítimo.
b. Cuando la base es el interés legítimo, el deber de transparencia resulta fortalecido, pues en la información facilitada se deben especificar los intereses legítimos concretos del responsable o del tercero que justifican el tratamiento, tanto si los datos se han obtenido directamente del interesado como si no ha sido así (arts. 13.1.d y 14.2.b RGPD). Adicionalmente, se le concede al interesado derecho a oponerse en cualquier momento al tratamiento de datos personales por motivos relacionados con su situación personal, debiendo el responsable dejar de tratar los datos personales salvo que acredite "motivos legítimos imperiosos" que preva-

[41] A propósito de ello, advierte el GT29 en su documento *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, adoptadas el 28 de noviembre de 2017 y revisadas el 10 de abril de 2018, p. 26: «Es importante señalar en este punto que, si un responsable del tratamiento elige basarse en el consentimiento para cualquier parte del tratamiento, deberá estar preparado para respetar dicha opción y detener esa parte del tratamiento si una persona retira su consentimiento. Enviar el mensaje de que los datos se tratarán sobre la base del consentimiento, mientras en realidad, se está utilizando otra base jurídica, sería realmente desleal para con los interesados. Con otras palabras, el responsable no puede pasar del consentimiento a otras bases jurídicas. Por ejemplo, no le está permitido utilizar retrospectivamente la base del interés legítimo con el fin de justificar el tratamiento, cuando se encuentre con problemas con la validez del consentimiento. Debido al requisito de divulgar la base jurídica utilizada por el responsable del tratamiento en el momento de la recogida de los datos personales, los responsables deben decidir cuál es la base jurídica aplicable antes de recoger los datos. »

lezcan sobre los intereses, derechos y libertades del afectado (art. 21.1 RGPD), así como el más concreto a no ser objeto de una decisión, que evalúe aspectos personales relativos a él, y se base únicamente en el tratamiento automatizado. Pero no entra en juego el derecho a la portabilidad de los datos, ni el de supresión, salvo, en este último caso, que los datos ya no fueran necesarios en relación con los fines del tratamiento, se haya ejercitado el derecho de oposición, hayan sido tratados ilícitamente, deban suprimirse en cumplimiento de una obligación legal o se trate de datos personales obtenidos en relación con la oferta de servicios de la sociedad de la información a menores (art. 17 RGPD).

25. Desde el prisma contractual, como se ha indicado más arriba, si la causa legitimadora del tratamiento es, por ejemplo, el consentimiento del titular de los datos-consumidor habría que analizar su delimitación e interacciones con el consentimiento contractual, así como la incidencia que su libre revocación *ex* artículo 7.3 RGPD pueda tener en la estabilidad contractual.

26. Partiendo de que la DCDig. (art. 2, núm. 8) asume el concepto de datos personales ampliamente delimitado por el artículo 4.1 RGPD[42], conviene distinguir entre:

- Datos facilitados por el consumidor para ser *tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales*.
- Datos facilitados por el consumidor para ser tratados exclusivamente por el empresario *con el fin cumplir sus obligaciones legales*
- Datos facilitados por el consumidor para ser tratados por el empresario *con otras finalidades a cambio de acceder a contenidos o servicios digitales*. No obstante, el art. 3.5.f DCDig. excluye de su ámbito de aplicación los contratos relativos a programas (software) ofrecidos por el empresario bajo una licencia gratuita o de código abierto, cuando el consumidor no pague ningún precio y *los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de mejorar la seguridad, compatibilidad o interoperabilidad de ese programa*[43] (software) concreto[44].

27. El tratamiento de los datos de los dos primeros grupos resulta claramente incardinable en las previsiones del artículo 6.1 RGPD, bien en su letra b) [datos tratados con el fin de suministrar los contenidos o servicios digitales y, por tanto, *necesarios para la ejecución de un contrato en el que el interesado es parte*], bien en su letra c) [tratamiento necesario para el *cumplimiento de una obligación legal aplicable al responsable*-empresario]. Mayores dudas e incertidumbres ofrece la fijación de la legitimación del tratamiento de aquellos datos facilitados por el consumidor para ser tratados por el empresario con finalidades distintas al suministro a cambio de acceder a contenidos o servicios digitales. Varias causas de licitud podrían hacerse valer, pero principalmente adquieren relevancia a estos efectos: la necesidad para la ejecución del contrato *ex* artículo 6.1.b RGPD (IV.1); el consentimiento *ex* artículo

[42] Art. 4.1) RGPD: «"datos personales": toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

[43] La razón de esta exclusión aparece explícita en el considerando 32 DCDig: eliminar trabas a esta evolución del mercado que puede contribuir a la investigación y la innovación en el mercado de los contenidos y servicios digitales.

[44] No abordaremos en este trabajo las cuestiones que suscita el tratamiento de datos personales en los contratos de compraventa de bienes con elementos digitales, en los que la ausencia del contenido o servicio digital incorporado o interconectado impediría que los bienes cumpliesen su función y en los que el contenido o servicio digital se facilita con los bienes en virtud de un contrato de compraventa relativo a esos bienes (reloj o televisor inteligente que únicamente puede cumplir sus funciones con una aplicación que se suministra en virtud del contrato de compraventa), ya sea el contenido o servicio digital incorporado o interconectado suministrado por el propio vendedor o por un tercero en virtud del contrato de compraventa. Contratos a los que resulta aplicable la Directiva (UE) 2019/771 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes, por la que se modifican el Reglamento (CE) 2017/2394 y la Directiva 2009/22/CE y se deroga la Directiva 1999/44/CE.

6.1.a (IV.2); el interés legítimo en los términos de la letra f del artículo 6.1 RGPD (IV.3); y las circunstancias señaladas en el artículo 9.2 RGPD para el tratamiento de datos de categoría especial (IV.4). A las bases legitimadoras que puedan ser aplicables a este tratamiento y su incidencia en el contrato de suministro se dedica el siguiente epígrafe.

IV. Bases legitimadoras del tratamiento de datos personales facilitados por el consumidor con fines distintos al suministro de contenidos o servicios digitales

1. Datos necesarios para la ejecución del contrato (art. 6.1.b RGPD)

28. Desde la perspectiva de la existencia de un contrato bilateral y de la ejecución de las obligaciones asumidas por cada una de las partes, cabría concluir que los datos del consumidor tratados por el empresario con finalidades distintas al suministro a cambio de acceder a contenidos o servicios digitales resultarían ser datos tratados lícitamente por ser necesarios para la ejecución del contrato[45], esto es, para la ejecución de la prestación asumida por el consumidor[46]. Ciertamente la redacción final de la DCDig., a diferencia de la Propuesta inicial de la Comisión Europea[47], ya no alude a "*otra contraprestación no dineraria en forma de datos personales"* pero, como advierte Navas Navarro, parece claro que sólo cuando el consumidor se comprometa a que sus datos sean utilizados para finalidades distintas al suministro, a modo de contraprestación por los contenidos digitales, será de aplicación la DCDig.; «de un modo conscientemente confuso y ambiguo, el texto sigue considerando que se pueden proporcionar datos personales en contraprestación por el suministro de contenido o de servicios digitales, si bien lo hace mediante una negación»[48]. Esa misma ambigüedad ha sido puesta de manifestado por el propio SEPD en su *Opinion 8/2018 on the legislative package "A New Deal for Consumers",* de 5 de octubre de 2018, en referencia a la redacción finalmente dada al artículo 3.1 DCDig., finalmente también incorporada a la Directiva 2011/83/UE, tras su modificación por la Directiva 2019/2161/UE [49].

---

[45] Vid. R. Martínez Martínez: "¿Consentimiento o contrato?", en http://lopdyseguridad.es/consentimiento-o-contrato/ 1 de junio de 2018.

[46] Desde esta perspectiva siguiendo a De Franceschi (*op. cit*., pp. 82-83) resulta interesante plantearse hasta cuándo cedemos nuestros datos, o qué cantidad de datos aceptamos ceder en contraprestación por determinados bienes o servicios en la economía digital. Señala el autor que si observamos las cláusulas de aceptación al tratamiento de datos veremos que se expresan en términos muy genéricos ("acepto compartir mis datos"); esta imprecisión (indeterminación de la prestación) que aceptamos con total normalidad en lo que se refiere al consentimiento en el tratamiento de datos podría afectar, cuando los datos sirven como contraprestación en un contrato sinalagmático, a la determinación de uno de los objetos sobre los que dicho contrato recae (en concreto, el precio): si los datos son utilizados como sustitutito del pago monetario ("valor comparable al dinero"), sería tanto como decir en un contrato de compraventa "acepto pagar dinero por este bien", sin especificar cuánto.

[47] Sobre la Propuesta de Directiva inicial, vid. G. Spindler: "Contratos de suministro de contenidos digitales: ámbito de aplicación y visión general de la Propuesta de Directiva de 9.12.2015", *Indret: Revista para el Análisis del Derecho,* Barcelona, julio 2016, pp. 1-17; S. Cámara Lapuente, "El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015", *Indret: Revista para el Análisis del Derecho,* Barcelona, julio 2016, pp. 1-91; J. Plaza Penadés, "Contract for the Supply of Digital Content", en J. Plaza Penadés y L. M. Martínez Velencoso (Eds.), *European Perspectives on the Common European Sales Law*, Springer, 2015, pp. 207-224; R. Schulze, "Nuevos retos para el Derecho de contratos europeo y cuestiones específicas acerca de la regulación del suministro de contenidos digitales", en E. Arroyo Amayuelas y Á. Serrano de Nicolás (Dirs.), *La europeización del Derecho privado: cuestiones actuales*, Marcial Pons, Madrid, 2016, pp. 15-27 y "La protección de los consumidores en la contratación digital", Conferencia pronunciada el 24 de mayo de 2018 en la Academia Matritense del Notariado, accesible en http://www.cnotarial-madrid.org/nv1024/paginas/tomos_academia/058-18-dig-anales_58-14-reiner_schulze.pdf, reseñada en *El Notario del Siglo XXI*, septiembre-octubre, Nº 81, 2018; J. A. Castillo Parrilla, "El contrato de suministro de contenidos digitales y los contratos de desarrollo de software y creación web en el derecho de consumidores. De la propuesta CESL y la Directiva 2011/83/UE a la propuesta de Directiva 634/2015, de 9 de diciembre", *Revista CESCO de Derecho de Consumo*, Nº 17, 2016, pp. 45-61.

[48] Así, S. Navas Navarro: "Datos personales y mercado", en Id. (Coord.) *Inteligencia artificial. Tecnología. Derecho*, Tirant lo blanch, Valencia, 2017, p. 262.

[49] SEPD: *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, 5 de octubre de 2018, p. 13: «La Propuesta ha tenido en cuenta las recomendaciones incluidas en el Dictamen 4/2017 del SEPD y evita usar el término «contraprestación» y distinguir entre los datos proporcionados por los consumidores de manera «activa» o «pasiva» a los proveedores de contenidos digitales. Sin embargo, el SEPD observa con preocupación que las nuevas definiciones previstas en la Propuesta introducirían el concepto de contratos de suministro de contenido digital o servicios digitales por los que los consumidores pue-

29. Desde esta óptica, considerando los datos facilitados para finalidades distintas al suministro como "*necesarios para la ejecución del contrato*", el propio consentimiento contractual legitimaría al proveedor para el tratamiento de los datos personales proporcionados por el consumidor, no siendo procedente justificar tal tratamiento de datos en el consentimiento del consumidor-interesado *ex* artículo 6.1.a RGPD[50]. Este tratamiento de datos personales del consumidor mantendría su vigencia durante toda la relación contractual, quedando sin efecto sólo cuando una norma aplicable al contrato o el propio contenido contractual prevean su revocación (a diferencia de la libre revocabilidad del tratamiento de datos basado en el consentimiento conforme al RGPD –art. 7.3-)[51].

30. No obstante, esta interpretación del artículo 6.1.b que derivaría de la DCDig.[52] está en abierta contradicción con la realizada por las autoridades europeas en materia de protección de datos, que abogan por una interpretación unilateral, esto es, datos necesarios para la ejecución del contrato pero desde la perspectiva del cumplimiento de las obligaciones asumidas por el proveedor de contenido o prestador del servicio.

— Primero fue el Grupo de Trabajo del artículo 29 (GT29) que, en su *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*, de 9 de abril de 2014, consideró que: a) El criterio de "necesidad" requiere una relación directa y objetiva entre el propio tratamiento y el propósito de la relación contractual que espera el interesado titular de los datos; b) No comprende situaciones en las que el tratamiento no sea realmente necesario para la ejecución de un contrato, sino unilateralmente impuesto al interesado por parte del responsable del tratamiento.
— Esta interpretación estricta y unilateral es la que parece consolidarse tras el RGPD. El pasado mes de abril, el Comité Europeo de Protección de Datos (CEPD), que sustituye al GT29, lanzaba a consulta pública un borrador, finalmente adoptado en octubre y publicado como *Guía 2/2019 para el tratamiento de datos personales conforme al artículo 6.1.b) en el contexto de los servicios en línea*[53]*,* que interpreta el concepto de "necesidad" en el contexto contractual siguiendo las directrices argumentativas del GT29. A tales efectos, advierte de la

---

den «pagar» con sus datos personales en lugar de hacerlo con dinero. Este nuevo planteamiento no solucionaría los problemas ocasionados por el uso del término «contraprestación» ni por la analogía entre el suministro de datos personales y la satisfacción de un pago dinerario. En concreto, al concebir los datos personales como un mero activo económico, este planteamiento no tiene en cuenta el carácter de derecho fundamental que tiene la protección de datos […]. En consecuencia, el SEPD recomienda que se eviten las referencias a los datos personales en las definiciones de «contrato de suministro de contenido digital que no se facilita en un soporte material» y «contrato de servicios digitales» y sugiere que, en su lugar, se utilice un concepto de contrato en virtud del cual el comerciante suministre o se comprometa a suministrar unos contenidos digitales específicos o un servicio digital a los consumidores *"*independientemente de si a estos se les requiere su *pago"*».

[50] En este sentido, vid. S. Navas Navarro, *op. cit*., pp.. 260-263, quien señala: «El consentimienro dado por el titular es un consentimiento contractual, la finalidad o finalidades para la cual sus datos son tratados un motivo causalizado y, si el consumidor retira su consentimiento, incumple, salvo que se hubiese pactado una facultad de desistir».

[51] Partiendo de su consideración como contraprestación pero basando el tratamiento de datos personales del consumidor en el consentimiento y no en la ejecución del contrato, L. M. Martínez Velencoso y M. Sancho López ("El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?", *Indret: Revista para el Análisis del Derecho,* enero 2018, p. 11) abordan la naturaleza de la oblicación asumida, indicando: «En el caso de la cesión de datos personales a cambio de contenidos digitales, tratándose de derechos de la personalidad, el titular del derecho sobre su información personal no puede transmitir el mismo en su totalidad ni constituir titularidades sobre las facultades que integran el derecho. Puede, sin embargo, autorizar el acceso a su esfera de exclusividad. La autorización no crea ninguna titularidad jurídica en el tercero, pero confiere licitud al acceso, independientemente de las razones que impulsen al autorizante y al autorizado. En mi opinión, el cedente de los datos asume una obligación de hacer, en concreto una obligación de cesión de uso de la información, del que la otra parte puede obtener un rédito. Ello de modo semejante a los contratos de cesión de los derechos sobre la imagen, siendo posible la cesión a terceros de la explotación comercial de la misma, siempre dentro de unos límites temporales y con la posibilidad de revocar el consentimiento en cualquier momento (v. gr. un contrato oneroso) ».

[52] R. Robert y L. Smit, *op. cit*., pp. 167-168.

[53] Comité Europeo de Protección de Datos (CEPD): *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject,* adoptada el 8 de octubre de 2019, accesible en https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_es.

obligación de los responsables de evitar cualquier confusión sobre cuál sea la base legal aplicable y destaca que la determinación de un tratamiento como "*necesario para la ejecución de un contrato*" no implica solamente evaluar el contenido contractual sino analizar también si el tratamiento es necesario para alcanzar el objetivo perseguido por el titular de los datos y si el servicio puede prestarse o ser ejecutado sin el tratamiento en cuestión; e, incluso, constando el contrato de varios servicios, señala que la aplicabilidad del artículo 6.1.b RGPD debe evaluarse respecto de cada uno de esos servicios por separado, determinando lo que es objetivamente necesario para realizar cada uno de los servicios que el interesado ha solicitado. Reconoce asimismo que el simple hecho de hacer referencia o mencionar el tratamiento de datos en un contrato, especialmente cuando es impuesto unilateralmente por el responsable, no es suficiente darle cobertura o licitud con base en esta causa de legitimación[54]. A reglón seguido, el CEPD analiza la aplicabilidad o no del art. 6.1.b RGPD a determinados tratamientos como los efectuados con el fin de mejorar el servicio, la prevención del fraude, la publicidad comportamental en línea o la personalización de contenidos, respecto de los que considera, con carácter general, no resultarles de aplicación la norma; sólo en algunos casos (mejora del servicio, personalización del contenido), cuando esa finalidad constituya un elemento esencial o intrínseco al propio servicio en línea contratado, cabe legitimar su tratamiento en apartado b) del artículo 6.1 RGPD. Por otra parte, es taxativo al afirmar, siguiendo al SEPD, que «los datos personales no pueden ser considerados como un producto comercializable». Insistiendo en que, aún cuando cualquier interesado puede aceptar el tratamiento de sus datos personales (y a tal efecto hace alusión expresa a la DCDig.), «no puede canjear o intercambiar sus derechos fundamentales mediante un contrato»[55].

2. Consentimiento del consumidor (art. 6.1.a RGPD)

31. Desde otra perspectiva, más acorde con la visión predominante en el ámbito europeo, contraria a reconocer que la autorización del consumidor para el acceso y tratamiento de su información con finalidades distintas al suministro del contenido o servicio digital puede configurarse como una contraprestación no dineraria[56], la base legitimadora debería ser otra de las mencionadas en el artículo 6 RGPD. No resultando aplicable ni el cumplimiento de una obligación legal (art. 6.1.c RGPD), ni la protección de intereses vitales (art. 6.1.d RGPD), ni el cumplimiento de una misión realizada en interés público o el ejercicio de poderes públicos conferidos al responsable (art. 6.1.e RGPD), se acude, prevalentemente, al consentimiento del interesado para el tratamiento de sus datos personales para uno o varios fines específicos, conforme al artículo 6.1.a RGPD[57].

---

[54] Gráficamente, el CEPD considera que la respuesta a las siguientes preguntas pueden servir de orientación a los responsables a la hora de evaluar la aplicación del artíulo 6.1.b RGPD: a) ¿Cuál es la naturaleza del servicio que se brinda al interesado? ¿Cuáles son sus características distintivas?; b) ¿Cuál es el fundamento exacto del contrato (es decir, su sustancia y objeto fundamental)?; c) ¿Cuáles son los elementos esenciales del contrato?; d) ¿Cuáles son las perspectivas y expectativas mutuas de las partes del contrato? ¿Cómo se promociona o anuncia el servicio al interesado? ¿Un usuario ordinario del servicio esperaría razonablemente que, teniendo en cuenta la naturaleza del servicio, el tratamiento previsto se llevará a cabo para ejecutar el contrato del que es parte?.

[55] El CEPD considera que existen, además, «razones adicionales por las que el tratamiento de datos personales es conceptualmente diferente de los pagos monetarios. Por ejemplo, el dinero es contable, lo que significa que los precios se pueden comparar en un mercado competitivo, y los pagos monetarios normalmente solo se pueden hacer con la participación del interesado. Además, los datos personales pueden ser explotados por varios servicios al mismo tiempo. Una vez que se ha perdido el control sobre los datos personales, ese control no necesariamente se puede recuperar».

[56] A propósito de la intransmisibilidad de la información personal y de su enfoque "propietario", cfr. M. R. Llácer matacás, *op. cit*., pp. 48-59.

[57] Como puede comprobarse del análisis de las expresiones contenidas en las políticas de privacidad de los principales proveedores de contenidos y servicios digitales, la base legitimadora del consentimiento es utilizada de manera diferente:

– *Google* (https://policies.google.com/privacy): «*Google* solicita tu autorización para tratar tu información con unas finalidades determinadas, y tienes derecho a revocar tu consentimiento en cualquier momento. Por ejemplo, se te pide tu consentimiento para proporcionarte servicios personalizados, como anuncios basados en tus intereses. También pedimos tu consentimiento cuando recogemos tu actividad de voz y audio para el reconocimiento de voz.» La plataforma alude al

32. Ahora bien, en tal caso debe distinguirse claramente el consentimiento contractual del consumidor de su consentimiento para el tratamiento de sus datos personales, lo que con frecuencia no suele producirse en el contexto de los contratos de suministro de contenidos y servicios digitales en los que los clausulados ligan ambos consentimientos[58]. Como reiteradamente advierten las autoridades europeas debe evitarse cualquier confusión al respecto. Así el SEPD, en su ya citada *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, alerta del error al que puede inducir el concepto de «contratos de suministro de contenido digital o servicios digitales por los que los consumidores facilitan sus datos personales en lugar de realizar un pago dinerario», dado que los proveedores de servicios pueden considerar que mediando el consentimiento en el contexto de un contrato se cumpliría la normativa en todos los casos, incluso cuando no se dieran las condiciones para el consentimiento válido previstas en el RGPD. Del mismo modo, el CEPD, en su reciente *Guía 2/2019 para el tratamiento de datos personales conforme al artículo 6.1.b) en el contexto de los servicios en línea*, aboga por evitar cualquier confusión sobre cuál sea la base legal aplicable cuando se suscribe un contrato: «Dependiendo de las circunstancias, los interesados pueden tener la impresión errónea de que están dando su consentimiento de conformidad con el Artículo 6 (1) (a) al firmar un contrato o aceptar los términos del servicio. Al mismo tiempo, un controlador puede asumir erróneamente que la firma de un contrato corresponde a un consentimiento en el sentido del artículo 6 (1) (a). Estos son conceptos completamente diferentes. Es importante distinguir entre aceptar los términos del servicio para celebrar un contrato y dar su consentimiento en el sentido del Artículo 6 (1) (a), ya que estos conceptos tienen diferentes requisitos y consecuencias legales».

---

consentimiento para compartir información con empresas, organizaciones o individuos ajenos: «compartiremos información personal de forma externa a *Google* si contamos con tu consentimiento. Por ejemplo, si utilizas *Google Home* para hacer una reserva a través de un servicio de reservas, te pediremos permiso antes de compartir tu nombre o número de teléfono con el restaurante. Te solicitaremos tu consentimiento explícito para compartir cualquier información personal sensible.»

- *Apple* (https://www.apple.com/es/legal/privacy/es/) efectúa una declaración genérica sin concretar ni conectar base legitimadora y finalidad, remitiendo a contactar con el Delegado de Protección de Datos para cualquier consulta al respecto: «Podemos procesar tus datos de carácter personal: para los fines descritos en esta Política de Privacidad, con tu consentimiento, para cumplir con un mandato legal al que esté sujeto *Apple,* para cumplir un contrato del que tú formas parte, para proteger tus intereses vitales, o si consideramos que es necesario para los intereses legítimos de *Apple* o un tercero al que haya que revelar información. Si tienes preguntas sobre esta base legal, puedes contactar con el Delegado de Protección de Datos europeo. »
- *Facebook* e *Instagram* (https://www.facebook.com/about/privacy/legal_bases): «En ciertos casos, nos adherimos a las bases jurídicas siguientes a la hora de tratar tus datos. Tu consentimiento: Para tratar datos de categorías especiales (como creencias religiosas, ideologías políticas, qué personas te interesan o información sobre tu salud, si compartes estos datos en los acontecimientos importantes o los distintos campos de tu perfil de *Facebook*), de modo que podamos compartirlos con quien determines y personalizar tu contenido; Para usar tecnología de reconocimiento facial; Para usar los datos que los anunciantes y otros socios nos proporcionen sobre tu actividad fuera de los productos de las empresas de *Facebook*, de modo que podamos personalizar los anuncios que te mostramos en dichos productos, así como en los sitios web, las aplicaciones y los dispositivos en los que se emplean nuestros servicios publicitarios; Para compartir con los anunciantes datos que te identifiquen personalmente (como tu nombre o dirección de correo electrónico; elementos que, por sí solos, pueden facilitar una vía de contacto o revelar tu identidad), como cuando nos indicas que compartamos tu información de contacto con un anunciante para que pueda enviarte, por ejemplo, información adicional sobre un producto o servicio promocionado; Para recopilar la información que nos autorices a recibir a través de la configuración que apliques en tus dispositivos (como permitir el acceso a tu ubicación de GPS, tu cámara o tus fotos), de modo que podamos ofrecerte las funciones y los servicios descritos al activar estos ajustes.»
- *Spotify* (https://www.spotify.com/es/legal/privacy-policy/) alude al consentimiento y al interés legítimo para «comunicarse con usted, ya sea directamente o a través de uno de nuestros socios, para: marketing, investigación, participación en encuestas, concursos, sorteos y promociones, a través de mensajes de correo electrónico, notificaciones u otros mensajes, conforme a los permisos que puede habernos comunicado (p. ej., a través de la página Configuración de cuenta)». Y solo al consentimiento para «ofrecerle funciones, información, publicidad o cualquier otro contenido que se base en su ubicación específica.»
- *Dropbox* (https://help.dropbox.com/es-es/accounts-billing/security/privacy-policy-faq) recoge como finalidades de procesamiento de datos personales con base en el consentimiento las siguientes:
  - «Enviarte material de marketing sobre nuestros Servicios. Si no deseas recibir este material, haz clic en el enlace Cancelar suscripción en cualquier mensaje de correo electrónico o actualiza tus preferencias en la sección Notificaciones de tu cuenta de Dropbox.
  - Conectar tu cuenta de Dropbox con otros servicios de terceros a través de las API de *Dropbox.*
  - Recopilar tus comentarios para mejorar nuestros Servicios y desarrollar nuevas funciones.»

[58] En ocasiones, se advierte que el bloqueo de *cookies* impedirá el uso total o parcial del servicio o que la revocación del consentimiento al tratamiento de ciertos datos sólo puede hacerse con la extinción del contrato o conllevará la desactivación o cancelación de la cuenta.

33. Siendo el consentimiento del interesado-consumidor *ex* artículo 6.1.a RGPD la base de legitimación del tratamiento, las consecuencias desde la óptica contractual serían considerar el contrato de suministro como gratuito, no oneroso, pero sujeto al cumplimiento, por parte del consumidor, de una condición de Derecho público: el consentimiento para el tratamiento de sus datos personales; consentimiento que difiere del proporcionado al aceptar las condiciones o términos del servicio (que permanece dentro del contrato)[59]. Desde esta perspectiva, deberán observarse las exigencias para la emisión de un consentimiento válido tal y como advierte el considerando 38 DCDig.: «Cuando el tratamiento de datos personales esté basado en el consentimiento, en particular con arreglo al artículo 6, apartado 1, letra a), del Reglamento (UE) 2016/679, son de aplicación las disposiciones específicas de dicho Reglamento, incluidas las relativas a las condiciones para valorar si el consentimiento se presta libremente. La presente Directiva no debe regular la validez del consentimiento prestado».

34. Sin embargo, a mi modo de ver, el refuerzo y contundencia que al consentimiento, como título legitimador del tratamiento de datos, ha dado el RGPD no se ajustan del todo bien al modelo de negocio basado en el acceso a datos personales del consumidor para suministrarle contenidos o servicios digitales, especialmente en situaciones de asimetría contractual. Las fricciones están servidas. El estándar más exigente del consentimiento configurado como «*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 persona*les que le conciernen*» (art. 4, núm. 11 RGPD), así como su revocabilidad en cualquier momento, casan mal con la dinámica de los contratos de suministro de contenidos y servicios digitales; especialmente queda en entredicho el atributo de "libertad" y lo dispuesto en los apartados 2 y 4 del artículo 7 y considerandos 42 y 43 RGPD, tal y como han sido interpretados por el GT29 en sus *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*[60].

35. Veamos algunas de estas interferencias. Según resulta de la normativa de protección de datos, el consentimiento válido para el tratamiento de datos personales, además de estar precedido de una información suficiente, concisa, transparente, inteligible y de fácil acceso, debe reunir los siguientes caracteres:

— **Inequívoco y afirmativo**. El RGPD requiere una declaración del interesado o una clara acción afirmativa como forma de manifestación del consentimiento, lo que significa que siempre debe darse el consentimiento mediante una acción o declaración. Se trata, pues, de una voluntad manifestada de forma unívoca mediante una conducta activa. A propósito de ello, el GT29 advierte que «un responsable del tratamiento debe tener también en cuenta que el consentimiento no puede obtenerse mediante la misma acción por la que el usuario acuerda un contrato o acepta los términos y condiciones generales de un servicio. La aceptación global de los términos y condiciones generales no puede considerarse una clara acción afirmativa destinada a dar el consentimiento al uso de datos personales»[61]. Esta última es una práctica hoy día muy habitual en el suministro de contenidos y servicios digitales.

— **Separado**. El consentimiento debe obtenerse de forma separada del resto de términos y condiciones. El artículo 7.2 RGPD establece la necesidad de que, 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 deba presentarse de tal forma que se distinga claramente

[59] Así, R. Mańko y S. Monteleone: *Contracts for the supply of digital content and personal data protection*. *European Parliamentary Research Service*. Mayo 2017, pág. 8. En este mismo sentido se pronunciaron la Comisión de Mercado Interior y Protección del Consumidor y la Comisión de Asuntos Jurídicos, el 21 de noviembre de 2017, en su informe conjunto a la Propuesta de DCDig.: la norma sería aplicable a los contratos en los que el consumidor paga un precio y a los contratos en los que el contenido o servicio digital se suministra «bajo la condición de que el consumidor o el tercero recopilen datos personales en el interés del comerciante».

[60] GT29: *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, adoptadas el 28 de noviembre de 2017 y revisadas el 10 de abril de 2018. Documento accesible en https://ec.europa.eu/newsroom/article29/news-overview.cfm.

[61] GT29: *Directrices sobre el consentimiento…, cit.,* pág. 18.

de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. En este aspecto, el GT29 es claro**:** «*Si el consentimiento está incluido como una parte no negociable de las condiciones generales se asume que no se ha dado libremente*. En consecuencia, no se considerará que el consentimiento se ha prestado libremente si el interesado no puede negar o retirar su consentimiento sin perjuicio»[62]. Algo que igualmente es práctica habitual en el mercado digital.

— **Granular**. El consentimiento debe solicitarse de forma selectiva e independiente para cada uno de los distintos tratamientos y finalidades. El Considerando 32 RGPD señala 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 este mismo sentido artículo 6.2 LOPDGDD: «*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*».

— **Sin condicionalidad.** Por otra parte, el artículo 7.4 RGPD advierte que para evaluar si el consentimiento se ha otorgado libremente se tendrá en cuenta el hecho de que la ejecución de un contrato, o la prestación de un servicio, se haya condicionado a la autorización de un tratamiento de datos que no sea necesario para el cumplimiento del mencionado contrato. En este mismo sentido artículo 6.3 LOPDGDD: «*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 condicionalidad crea, pues, una presunción fuerte de falta de libertad. Lo que se refiere, como indica el GT29, a que se deba prestar atención, a si, entre otras, se produce alguna situación en la que el consentimiento esté «agrupado» (bundling) con la aceptación de términos y condiciones o «atado» a la provisión de un contrato o un servicio cuando los datos personales solicitado no son necesarios para el cumplimiento del contrato o la prestación de servicio. Según explica el GT29, el RGPD quiere asegurarse de que el tratamiento de los datos personales para los que se requiere el consentimiento del interesado no se convierta, directa o indirectamente, en la contraprestación del contrato. El propio GT29 establece que la condicionalidad quedará eliminada cuando el responsable del tratamiento ofrezca a los interesados *una elección real*, esto es, si estos pudieran escoger entre un servicio que incluya el consentimiento para el uso de datos personales con fines adicionales y un servicio equivalente ofrecido por el mismo responsable que no implicara prestar el consentimiento para el uso de datos con fines adicionales. Siempre que exista una posibilidad de que dicho responsable del tratamiento ejecute el contrato o preste los servicios contratados sin el consentimiento para el otro uso o el uso adicional de los datos en cuestión, significará que ya no hay condicionalidad con respecto al servicio. No obstante, ambos servicios deben ser realmente equivalentes. Por tanto, puede concluirse que, cuando se solicita el consentimiento como condición previa de (y no relacionada con) el servicio que se presta, si el tratamiento no puede basarse en otra causa (p. ejem., interés legítimo), aunque se preste el consentimiento, éste seguramente será inválido, al no haberse prestado con plena libertad[63]. En este mismo sentido la Agencia Española de Protección de Datos (AEPD), en una reciente *Nota técnica sobre el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles*, de 17 de septiembre de 2019, indica: «la instalación y utilización de la app no puede estar condicionada a la obtención de un consentimiento para un tratamiento no necesario para proporcionar el servicio definido en la misma»[64].

— **No desequilibrio:** No procede en un contexto de predominio del responsable frente al titular de los datos**.** El considerando 43 RGPD, recogiendo esta idea, va más allá al precisar que,

[62] GT29: *Directrices sobre el consentimiento…, cit.,* pág. 6.

[63] GT29: *Directrices sobre el consentimiento…, cit.,* págs. 8-10.

[64] Accesible en: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf

para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido en un caso particular cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento, lo que lleva a plantearse si realmente el consentimiento es libre en ámbitos como el nos ocupa caracterizado por el "o lo tomas o lo dejas", con predominio de clausulados en los que existe una predisposición contractual por parte del empresario, limitándose el consumidor a aceptarlo. Como ha expresado el GT29, pueden existir supuestos en los que se produzca un desequilibrio entre las partes y en los que, para que el consentimiento sea válido, lo esencial será permitir que el interesado pueda ejercer una elección real, sin que haya riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta[65].

— **Ausencia de perjuicio**. En todo caso, tal y como resulta del considerando 42 RGPD, el consentimiento no se considerará libremente prestado, no sólo cuando el interesado no goza de verdadera o libre elección, sino también cuando no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno[66].

— **Revocable.** Finalmente, «el interesado tendrá derecho a retirar su consentimiento en cualquier momento» (art.7.3 RGPD), aunque tal revocación no afectará al tratamiento de datos realizado con anterioridad.

36. Esta última característica del consentimiento, su revocabilidad, constituye todo un desafío para el Derecho contractual[67] por varias razones:

i. En primer lugar, el carácter revocable del consentimiento supone dejar sin efecto la amplia excepción al desistimiento en los contratos de suministro de contenidos y servicios digitales prevista en el artículo 103, letras a) y m) del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU) para los contratos a distancia de prestación de servicios o de suministro de contenido digital[68], dado que el consumidor titular de los datos siempre podría desvincularse del contrato revocando su consentimiento al tratamiento, por lo que gozaría de un derecho de desistimiento unilateral *ad nutum sine die* respecto del propio vínculo contractual que no tendría el consumidor que ha abonado una contraprestación dineraria[69].

---

[65] GT29: *Directrices sobre el consentimiento…, cit.,* pág. 11-12.

[66] Lo cierto es, como advierte J. Herrero García ("Consentimiento Informado: Origen y solución de todos los problemas", en https://jorgegarciaherrero.com/consentimiento-informado-origen-y-solucion-de-todos-los-problemas/), resulta difícil aceptar como consentimiento válido el acto de pinchar un botón de "acepto" en internet, o "instalar" una aplicación sin información significativa y comprensible, que no es leída por el consumidor, con unas condiciones de uso y política de privacidad que vienen impuestas unilateralmente y que sólo otorgan la posibilidad de aceptar o rechazar sin poderse negociar o aceptar granularmente módulos del servicio y tratamiento de datos vinculados a los mismos.

[67] Desafío que, como advertía V. Mak en relación con la Propuesta de DCDig., no tiene en la norma una respuesta adecuada (vid. "The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content", en *Workshop for the (JURI) Committee on Legal Affairs, European Parliament: New rules for contracts in the digital environment, with the participation of EU National Parliaments*, Brussels, 17 febrero 2016, p. 9, accesible en http://www.europarl.europa.eu/cmsdata/98771/Mak.pdf).

[68] Conforme al art. 103.m TRLGDCU, en el suministro de contenidos digitales sin soporte material, el consumidor pierde el derecho al desistimiento cuando comience la ejecución "*con el previo consentimiento expreso del consumidor y usuario con el conocimiento por su parte de que en consecuencia pierde su derecho de desistimiento*" (incluso aunque el suministro no haya finalizado ni se haya "ejecutado completamente", en el caso de prestaciones digitales periódicas); por su parte, en el ámbito de los contratos de servicios (art. 103.a TRLGDCU) "*una vez que el servicio haya sido completamente ejecutado, cuando la ejecución haya comenzado con el previo consentimiento con previo consentimiento expreso del consumidor y usuario y con el reconocimiento por su parte de que es consciente de que, una vez que el contrato haya sido completamente ejecutado por el empresario, habrá perdido su derecho de desistimiento"*. Vid. S. Cámara Lapuente, "La nueva protección del consumidor de contenidos digitales tras la Ley 3/2014, de 27 de marzo", *Revista CESCO de Derecho de Consumo*, Nº 11, 2014, pp. 153 y ss.

[69] Los problemas en orden a aplicar la sanción prevista (falta de pago por el consumidor del contenido consumido o del servicio ejecutado) para los supuestos de pérdida del derecho a desistir, cuando el empresario no cumpla con el requisito relativo a obtener el consentimiento expreso previo del consumidor y su conocimiento de que perderá el derecho de desistimiento, han llevado al legislador europeo a limitar este requisito relativo al "consentimiento reforzado" sólo a los contratos de suministro

ii. En segundo lugar, el ejercicio de un derecho concedido por una norma legal imperativa (art. 7.3 RGPD) no podría, ni excluirse por una cláusula contractual (que sería nula) [70], ni su ejercicio ser constitutivo de incumplimiento contractual, por lo que no activaría los remedios previstos legal o contractualmente para tal hipótesis, ni determinaría responsabilidad a cargo del consumidor[71].

iii. En tercer lugar, la revocación del consentimiento para el tratamiento de datos personales no implicaría de suyo la revocación del consentimiento contractual, pero las consecuencias no pueden ser otras que la posibilidad por parte del suministrador de resolver el contrato, actuando esta revocación como de si una condición resolutoria se tratase, derivada del ejercicio derechos fundamentales que, aun sin pacto, no puede ser desconocida por las partes[72] (e integraría el contrato *ex* art. 1258 C.c.).

iv. Pero es más, tal revocación del consentimiento confronta claramente con el art. 1256 Código civil: «*La validez y cumplimiento de los contratos no puede dejarse al arbitrio de una de las partes, en la medida en que el cumplimiento de una parte del contrato queda al arbitrio de uno de los contratantes*» (el titular de los datos)[73]. En este sentido, para salvar este obstáculo, se ha advertido que «no debe confundirse "consentimiento libre" con "consentimiento irresponsable". Un consentimiento es libre cuando no ha sido emitido bajo coacción o amenaza (art. 1267 CC), y puede ser retirado en cualquier momento. Ahora bien, la retirada del consentimiento acarreará, con carácter general, consecuencias patrimoniales derivadas del posible incumplimiento del contrato y, en su caso, producción de daños y perjuicios. Sólo excepcionalmente y por un período breve de tiempo (contratos con consumidores y durante 14 días naturales) se permite el desistimiento unilateral *ad nutum*. No parece razonable extender esta excepción a todas aquellas situaciones en que se pague con datos, pues significaría aceptar que en un sector de la economía que crece exponencialmente se permite que una de las partes del contrato emita un consentimiento irresponsable, contraviniendo reglas tan básicas como, por ejemplo en España, el artículo 1256 CC»[74].

---

a cambio de precio (vid. artículo 16 Directiva 2011/83/UE, párrafo primero, letras a) y m) en su versión modificada por art. 4 Directiva 2019/2161/UE).

[70] Al no interferir la DCDig. en las normas nacionales relativas a la validez, nulidad o eficacia respecto de materias no contempladas en la misma, como advierten R. Mańko y S. Monteleone (*op. cit*., p. 6), las consecuencias de un contenido contractual infractor de una norma imperativa de Derecho público, como el RGPD o las normas nacionales de implementación de la Directiva de privacidad en las comunicaciones electrónicas, dependerán de las reglas de Derecho privado aplicables en cada sistema nacional (nulidad, anulabilidad, nulidad parcial..). Dada la incertidumbre legal que la pluralidad de soluciones nacionales puede entrañar, advierte el autor que, en la tramitación legislativa, el Parlamento propuso incluir una nueva norma (a semejanza de la prevista en materia de cláusulas abusivas) advirtiendo que las cláusulas contractuales contrarias al RGPD, serían no vinculantes para el consumidor, siendo en los demás el contrato "*obligatorio para las partes en los mismos términos, siempre que pueda subsistir sin dichas cláusula".* Esta es la opción adoptada por el legislador español: la contravención del RGPD por una cláusula contractual no significa la ineficacia del contrato de suministro digital en sí, sino sólo de esa cláusula (vid. S. Cámara Lapuente, "Extinción de los contratos sobre contenidos y servicios digitales...", *cit.*, p. 164).

[71] Así, C. Langhanke, y M. Schmidt-Kessel ("Consumer Data as Consideration", *Journal of European Consumer and Market Law, EuCML*, Issue 6/2015, p. 222), con dos excepciones, según estos autores: engaño del consumidor en cuanto a la continuidad de su consentimiento al tratamiento y carácter intempestivo de la revocación.

[72] Sobre este aspecto, vid. R. Mańko y S. Monteleone, *op. cit*., p. 10. En opinión de C. Langhanke y M. Schmidt-Kessel (*op. cit.,* p. 222), el suministrador en tales casos tendría derecho a resolver el contrato.

[73] Desde la consideración de los datos como contraprestación, De Franceschi (*op. cit*., pp. 116-120) advierte que, en una situación en la que los datos sirven como medio de pago y la revocación del consentimiento al tratamiento de dichos datos está exenta de todo perjuicio económico, la estabilidad del contrato estaría constamente en juego y derivaría en un riesgo, amparado por la propia norma, de enriquecimiento sin causa del titular de los datos. El autor se pregunta si en tal caso la revocación del consentimiento no podría dar lugar a la obligación de reembolso de su valor por el consumidor (no a abtenerse de utilizarlos y ponerlos a disposition del suministrador).

[74] Así se expresa J. A. Castillo Parrilla: "Derecho al patrimonio digital. Bienes digitales y datos como bienes", en A. Troncoso Reigada (Coord.), *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos,* trabajo en prensa, amablemente facilitado por el autor.

37. Otro complejo aspecto que plantea esta base jurídica del tratamiento de datos personales es cuál sea la incidencia en el contrato de suministro de un consentimiento del consumidor que no reúne los requisitos para ser válido conforme al artículo 6.1.a RGPD. Si la ilicitud del consentimiento *ex* RGPD incidiera en la eficacia del contrato celebrado, provocando su invalidez, esto conduciría a la inaplicación de la DCDig. y de todo su manto protector de los intereses del consumidor, beneficiando al proveedor del contenido o servicio digital que quedaría al margen de las responsabilidades contractuales derivadas de la DCDig. (considerando 48). No parece, y carecería de lógica, que el incumplimiento por el responsable del tratamiento (el suministrador) de las exigencias derivadas de la normativa de protección de datos deba beneficiar a quien provoca tal incumplimiento, privando al consumidor-interesado de remedios contractuales[75]. En nuestra opinión, convenientemente separados consentimiento contractual y consentimiento en el sentido del artículo 6.1.a RGPD en los contratos de suministro de contenidos y servicios digitales, la ilicitud del consentimiento del consumidor para el tratamiento de sus datos personales debe discurrir por caminos diferentes a la licitud o ilicitud del consentimiento contractual, sin interferir en la validez del contrato celebrado. Esto es, un consentimiento para el tratamiento de datos personales que no reúne los requisitos del RGPD para su validez no provoca, por sí solo, la invalidez del contrato de suministro.

38. Por último conviene hacer mención al tratamiento de datos personales de menores de edad basado en su consentimiento. En concreto**,** ¿cuáles serían las implicaciones respecto de menores de edad que acceden a contenidos y servicios digitales, pudiendo autorizar el tratamiento de sus datos personales por haber alcanzado la capacidad para ello, pero no la capacidad contractual necesaria para la celebración del contrato?[76]. Recordemos que el artículo 7 LOPDGDD, concreta y extiende la aplicación del artículo 8 RGPD[77], señalando, en relación con el consentimiento de los menores de edad, que solo podrá emitirse válidamente cuando sea mayor de catorce años, siendo necesario para el tratamiento de datos de menores de catorce años que conste «*el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.*»[78]. A tal efecto el responsable del tratamiento hará esfuerzos

[75] Vid. P. Hacker, "Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive" (May 21, 2019), en S. Lohsse, R. Schulze y D. Staudenmayer (eds.), *Data as Counter-Performance: Contract Law 2.0?*. Hart/Nomos (de próxima publicación), págs. 10-11, disponible en https://ssrn.com/abstract=3391772; y A. Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper N.º 8, *Forschungsinstituts für Recht und digitale Transformation* (2019), Humboldt-Universität zu Berlin , págs. 6-7, accesible en https://www.rewi.hu-berlin.de/de/lf/oe/rdt/pub.

[76] Conforme al artículo 1263 Cc: "No pueden prestar consentimiento: 1. Los menores no emancipados, salvo en aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes, y los relativos a bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales. 2. Los que tienen su capacidad modificada judicialmente, en los términos señalados por la resolución judicial". Vid. A. Piñar Real, "Capítulo XII. Tratamiento de datos de menores", en J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo privacidad*, Ed. Reus, 2016, pp. 187-204; N. Brito Izquierdo, "Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales", *Actualidad Civil*, N.º 5, Mayo 2018; y F. J. Durán Ruiz, "El tratamiento de los datos personales de los menores de edad en la nueva normativa de protección de datos", en M. C. García Garnica y N. Marchal Escalona (Dirs.), *Aproximación interdisciplinar a los retos actuales de protección de la infancia dentro y fuera de la familia*, Thomson Reuters Aranzadi, Cizur Menor, 2019, pp. 473-497.

[77] El artículo 8 RGPD, dedicado a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, parte de la válida prestación del consentimiento de los menores en este ámbito a partir de los 16 años de edad, pero deja libertad a los Estados miembros para fijar una edad inferior, siempre que no baje de los 13 años; por su parte el legislador español no sólo ha concretado la edad para la válida prestación del consentimiento por menores, sino que no ha restringido su ámbito de aplicación a los servicios de la sociedad de la información.

[78] Al margen de las previsiones relativas a la validez del consentimiento, los menores son objeto de atención especial tanto en el RGPD [considerandos 38, 58, 65, 75, principio de licitud (art. 6.1. f), transparencia (art. 12), derecho de supresión (art. 17.1), códigos de conducta (art. 42), funciones autoridades de control (art. 57.1.b), imposición de multas administrativas (art. 83)], como en la LOPDGDD [no solo en sede de los nuevos derechos digitales que la norma reconoce (arts. 84, 92, 97.2, disp. adic. 19ª y disp. final 10ª), sino en materia de protección de sus datos personales a efectos de someter el tratamiento de datos de menores de edad a una evaluación de impacto en la protección de datos (art. 28.2), imponer la necesidad de contar un delegado de protección de datos a centros docentes y federaciones deportivas (art. 34.1), e incidir en la determinación y graduación de las sanciones (arts. 73 y 76)].

razonables para verificar que el consentimiento para el tratamiento de datos personales fue dado por el titular de la patria potestad o tutela, teniendo en cuenta la tecnología disponible (art. 8.2 RGPD).

39. La DCDig. requiere para ser aplicada la celebración de un contrato válido sin prejuzgar los criterios nacionales de validez o eficacia contractual, por tanto, podría producirse la circunstancia de que, con arreglo al Derecho español, el contrato celebrado fuese anulado por falta de capacidad, no entrando en juego los remedios de la DCDig., sin perjuicio de contar, en relación con los contenidos que no sean datos personales, con los generales previstos por el ordenamiento español. No obstante, en este caso, ni siquiera el tratamiento de datos personales de menores realizado por el suministrador sería lícito, con las consecuencias que de ello puedan derivarse conforme a la normativa de protección de datos. Y ello porque, en virtud de la previsión incorporada en el apartado segundo del artículo 7.1 LOPDGDD, el consentimiento al tratamiento a partir de los 14 años edad no es una regla absoluta, dado que queda exceptuada en aquellos supuestos en que «*la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento*.»

3. Interés legítimo del responsable o de terceros (art. 6.1.f RGPD)

40. Un último recurso, en el marco de las causas legitimadoras recogidas en el artículo 6.1 RGPD, sería justificar el tratamiento con base en la necesidad de satisfacer intereses legítimos perseguidos por el suministrador de contenidos o servicios digitales 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 (art. 6.1.f RGPD). El interés legítimo es concepto indeterminado[79], responde a las razones que tiene un responsable del tratamiento, para recoger, almacenar o comunicar a terceros datos personales ajenos, que deberá ser lícito (es decir, conforme con la legislación nacional y europea aplicable), estar articulado con claridad, ser suficientemente específico, y representar un interés real y actual (es decir, no especulativo)[80].

[79] El GT29, en su *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*, adoptado el 9 de abril de 2014, advierte: «El concepto de "interés" es la implicación más amplia que el responsable del tratamiento pueda tener en el tratamiento, o el beneficio que este obtenga, o que la sociedad pueda obtener, del tratamiento. Este puede ser apremiante, claro o controvertido. Las situaciones a las que hace referencia el artículo 7, letra f), pueden variar, por tanto, del ejercicio de derechos fundamentales o la protección de intereses personales o sociales importantes a otros contextos menos obvios o incluso problemáticos». Los considerandos 47 a 49 RGPD ejemplifican, entre otros intereses legítimos, los siguientes: la prevención del fraude, siempre que se cumpla el principio de minimización; el marketing directo; las transmisiones de datos en grupos de empresas para fines administrativos internos como puede ser la centralización de datos de clientes o empleados; las transmisiones de datos para garantizar la seguridad de las redes (p.ej. a los equipos de respuesta a emergencias informáticas – CERT – o de respuesta a incidentes de seguridad informática – CSIRT–), para impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de denegación de servicio y daños a los sistemas informáticos y de comunicaciones electrónicas. Por su parte, el GT29, en el mencionado *Dictamen 06/2014*, recoge algunos contextos en los que puede apreciarse la concurrencia de intereses legítimos del responsable: el ejercicio del derecho de libertad de expresión o información; la prospección comercial y otras formas de comercialización o publicidad; la ejecución de demandas legales, incluido el cobro de deudas mediante procedimientos extrajudiciales; la prevención del fraude, uso indebido de servicios o blanqueo de dinero; la supervisión de los empleados con fines de seguridad o de gestión; los canales internos de denuncias; la seguridad física y la seguridad de la red; el tratamiento con fines históricos, científicos o estadísticos; el tratamiento con fines de investigación (incluida la investigación de mercado); reutilización de datos de fuentes públicas. Y también menciona ámbitos en los que pueden operar intereses legítimos de terceros como la publicación de datos con fines de transparencia y responsabilidad o la investigación histórica u otro tipo de investigación científica.

[80] Vid. GT29: *Dictamen 06/2014 sobre el concepto de interés legítimo, cit.,* p. 30. Sobre esta causa de legitimación se ha pronunciado en diferentes ocasiones el TJUE: Sentencia de 24 de noviembre de 2011, C-468/10 y C-460/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF*) y *Federación de Comercio Electrónico y Marketing Directo (FECEMD*), en la que analiza la normativa española de transposición del artículo 7, letra f) de la Directiva 95/46/CE; Sentencia de 13 de mayo de 2014, C131/12, Google Spain SL & Google Inc. vs Agencia Española de Protecccción de Datos (AEPD) & Mario Costeja González; Sentencia de 4 de mayo de 2017, C-13/16, *Rigas Satskime*, que fija cuáles son los requisitos para que

41. Esta base legitimadora podrá justificar el tratamiento de datos personales para determinadas finalidades (personalización de contenidos, prevención del fraude, envío comunicaciones de carácter promocional, publicidad dirigida y presentación de ofertas relevantes…), pero su indeterminación y limitaciones hacen que no sea la más conveniente en la mayor parte de los casos en los que se accede a contenidos y servicios digitales a cambio de datos, dado que no basta con la concurrencia de un interés legítimo sino que es necesario que prevalezca sobre los intereses, derechos o libertades fundamentales del interesado. Por tanto, será necesario realizar en cada caso concreto un juicio de ponderación para poder determinar la prevalencia o no del interés legítimo; ponderación que deberá tener en cuenta no sólo la incidencia del tratamiento en los derechos y libertades del afectado, sino también en sus propios intereses[81], y será especialmente cualificada cuando el afectado sea un menor. El considerando 47 RGPD pone en relación esta ponderación con las expectativas razonables de los interesados basadas en su relación con el responsable del tratamiento[82]: «tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable». No obstante, incluso en estos casos se indica que cabe apreciar la prevalencia de los intereses y derechos del afectado cuando se proceda al tratamiento de sus datos en circunstancias en que no espere razonablemente que vaya a realizarse un tratamiento ulterior[83]. Si realizada la ponderación entre ambos intereses, del responsable y de los interesados, el resultado es dudoso, cabe articular una serie de garantías adicionales, cuyo cumplimiento o concurrencia pueden acabar inclinando la balanza a favor de unos intereses u otros. El GT29, a título orientativo, menciona algunas posibles garantías adicionales, dirigidas a impedir un impacto indebido sobre los interesados:

i. Medidas técnicas y organizativas para garantizar que los datos no puedan utilizarse con el fin de adoptar medidas o emprender otras acciones en relación con las personas («separación funcional» como es, con frecuencia, el caso en el contexto científico);
ii. Uso extensivo de técnicas de anonimización;
iii. Agregación de datos;
iv. Tecnologías de protección de la intimidad, protección de la privacidad desde el diseño, evaluaciones del impacto relativo a la protección de datos y a la intimidad;
v. Aumento de la transparencia;
vi. Derecho general e incondicional de exclusión voluntaria;
vii. Portabilidad de los datos y medidas relacionadas para capacitar a los interesados.

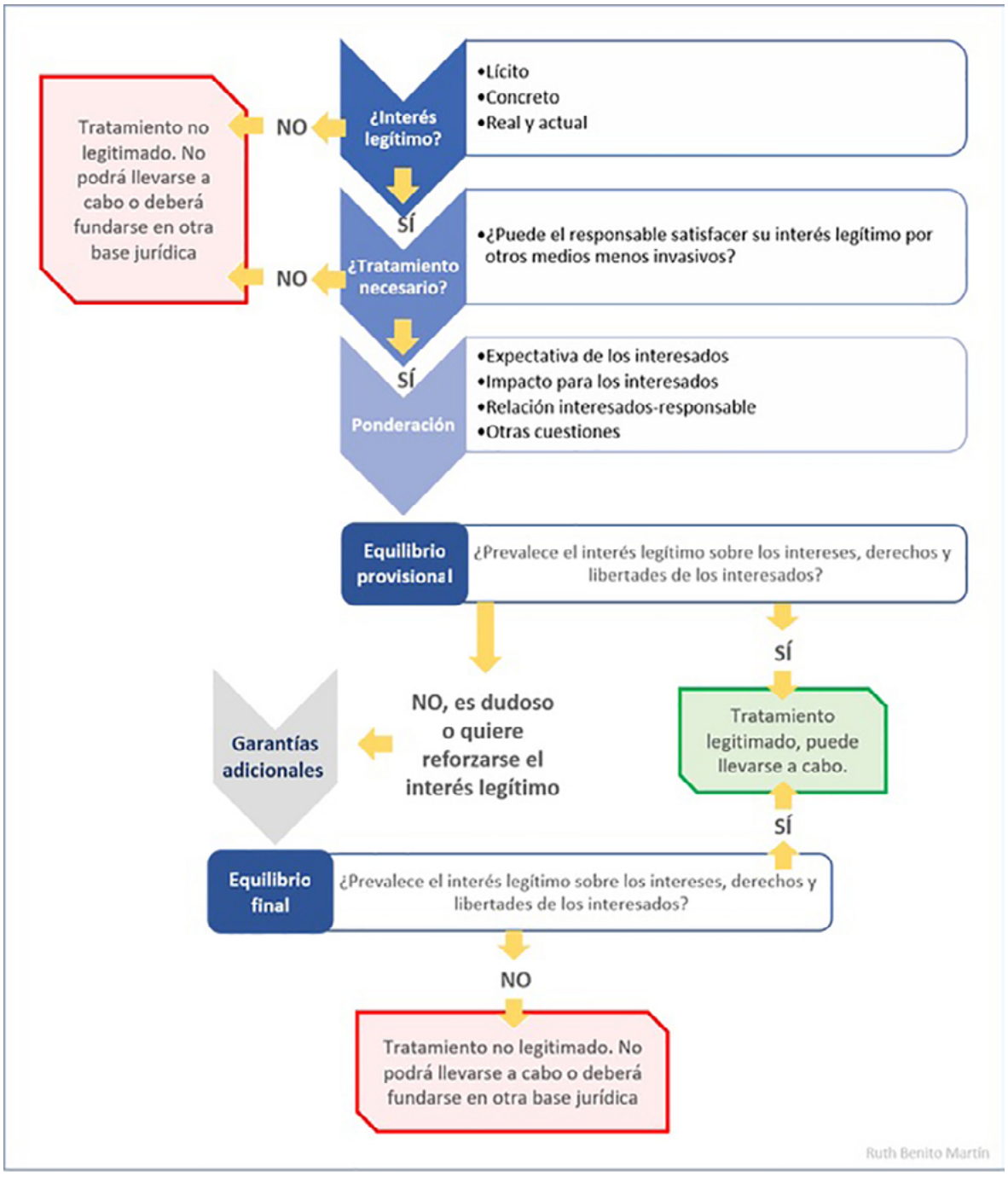
un tratamiento conforme al art. 7, letra f) de la Directiva 95/46/CE pueda resultar lícito; y, recientemente, Sentencia de 29 de julio de 2019, C-40/17, *Fashion ID GmbH & Co.KG vs. Verbraucherzentrale NRW eV*, que establece la necesidad, en caso de corresponsabilidad, de que cada responsable del tratamiento persiga un interés legítimo.

[81] «El concepto de "intereses" de los afectados se define incluso de manera más amplia, puesto que no requiere el elemento de "legitimidad". Si el responsable del tratamiento o la tercera parte pueden perseguir cualquier interés, siempre que no sea ilegítimo, el interesado a su vez tendrá derecho a que se tengan en cuenta todas las categorías de intereses que le afecten y a que se ponderen en relación con los intereses del responsable del tratamiento o la tercera parte» (así GT29, en su *Dictamen 06/2014)*.

[82] El GT29 (*Dictamen 06/2014*) advierte: «Los factores que deben considerarse cuando se efectúe dicha prueba de sopesamiento comprenderán: - la naturaleza y la fuente del interés legítimo, y si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, resulta de otro modo de interés público o se beneficia del reconocimiento de la comunidad afectada; - la repercusión para el interesado y sus expectativas razonables sobre qué sucederá con sus datos, así como la naturaleza de los datos y la manera en la que sean tramitados; - las garantías adicionales que podrían limitar un impacto indebido sobre el interesado, tales como la minimización de los datos, las tecnologías de protección de la intimidad, el aumento de la transparencia, el derecho general e incondicional de exclusión voluntaria y la portabilidad de los datos.»

[83] Además del *Dictamen 06/2014* del GT29 anteriomente mencionado, como señala F.J. Sempere Navarro, "Interés legítimo en el tratamiento de datos: análisis, ponderación y supuestos prácticos", *Privacidad Lógica*, 5 de marzo de 2019 (http://www.privacidadlogica.es/interes-legitimo-en-el-tratamiento-de-datos-analisis-ponderacion-y-supuestos-practicos/), otro documento aporta elementos de interés para realizar esta ponderación: la *Guía de la Autoridad de Protección de Datos de Reino Unido*, Information commissioner´s Oficce (ICO) de 2018, accesible en https://ico.org.uk/for-organisations/guide-to-data-protection/.

42. Ilustrativa resulta la siguiente infografía sobre los pasos a seguir para la determinación del interés legítimo como base legitimadora[84]:



[84] Realizada por R. Benito Martín: "Examen del interés legítimo como base del tratamiento de datos", *Blog Con la venia, señorías*, accesible en https://conlaveniasenorias.com/2017/08/31/examen-del-interes-legitimo-como-base-del-tratamiento-de-datos/, 31 de agosto de 2017.

43. El recurso al interés legítimo como base de licitud de determinadas finalidades del tratamiento de datos personales es frecuente en los clausulados y políticas de privacidad de los proveedores de contenidos digitales, como puede observarse en su empleo por algunas de las principales empresas proveedoras de prestaciones digitales: redes sociales (*Facebook* e *Instagram*/ *WhatsApp*[85]); descarga

[85] *Facebook - Instagram* (https://www.facebook.com/about/privacy/legal_bases) y WhatsApp (https://www.whatsapp.com/legal/?eea=1#how-we-process-your-information): «En ciertos casos, nos adherimos a las bases jurídicas siguientes a la hora de tratar tus datos: Nuestros intereses legítimos, o los de un tercero, en aquellos casos en los que no entren en conflicto con tus intereses o derechos y libertades fundamentales:

- En el caso de personas menores de edad (menores de 18 años en la mayoría de los países de la Unión Europea), cuya capacidad para formalizar un contrato válido es limitada, no podemos tratar sus datos personales aduciendo motivos de necesidad contractual. No obstante, cuando estas personas usan nuestros Servicios, nuestros intereses legítimos se basan en los fundamentos siguientes:
- Proporcionar, personalizar y mejorar los productos de *Facebook*. En el caso de personas que no hayan alcanzado la edad de consentimiento establecida en el estado miembro en el que residan, modificamos nuestros Productos de *Facebook* para garantizar la aplicación de protección especial y restringimos el acceso a ciertas funciones en relación con los datos que usamos para seleccionar los anuncios. Esto incluye el tratamiento de la información que las personas que no han alcanzado la edad de consentimiento nos autorizan a recibir a través de la configuración que aplican en sus dispositivos para proporcionar las funciones y los servicios a los que afectan dichos ajustes.
- Fomentar la seguridad, la integridad y la protección, incluido el uso de las herramientas específicas necesarias para luchar contra las amenazas que puedan acechar a las personas menores de edad.
- Facilitar vías de comunicación sin fines de comercialización para tratar los problemas que puedan surgir en relación con el servicio de atención al cliente y los productos.

Nuestros intereses legítimos a la hora de llevar a cabo el tratamiento de datos correspondiente se basan en los siguientes fundamentos:

- Crear, proporcionar, fomentar y mantener funciones y productos innovadores que permitan a los menores de edad expresarse, comunicarse, descubrir contenido, interactuar con la información y las comunidades que correspondan a sus intereses, crear comunidades y usar las herramientas y funciones que fomenten su bienestar.
- Mantener la seguridad de nuestra plataforma y nuestra red, verificar las cuentas y la actividad en estas, luchar contra las conductas perjudiciales, detectar y prevenir el spam y otras experiencias negativas, proteger los productos de las empresas de *Facebook* frente al contenido nocivo e inapropiado, investigar las actividades sospechosas y el incumplimiento de nuestras políticas y condiciones, y garantizar la seguridad de los menores de edad, tomando las medidas necesarias para impedir la explotación o cualquier otro tipo de daño ante el cual estas personas puedan ser particularmente vulnerables.
- Para todas las personas, incluidos los menores de edad:
- Para el aprovisionamiento de servicios de medición, análisis y de cualquier otro tipo para empresas, en los que somos responsables del tratamiento de los datos en calidad de controladores. Nuestros intereses legítimos a la hora de llevar a cabo el tratamiento de datos correspondiente se basan en los siguientes fundamentos:
- Crear, proporcionar, fomentar y mantener funciones y productos innovadores que permitan a los menores de edad expresarse, comunicarse, descubrir contenido, interactuar con la información y las comunidades que correspondan a sus intereses, crear comunidades y usar las herramientas y funciones que fomenten su bienestar.
- Mantener la seguridad de nuestra plataforma y nuestra red, verificar las cuentas y la actividad en estas, luchar contra las conductas perjudiciales, detectar y prevenir el spam y otras experiencias negativas, proteger los productos de las empresas de *Facebook* frente al contenido nocivo e inapropiado, investigar las actividades sospechosas y el incumplimiento de nuestras políticas y condiciones, y garantizar la seguridad de los menores de edad, tomando las medidas necesarias para impedir la explotación o cualquier otro tipo de daño ante el cual estas personas puedan ser particularmente vulnerables.
- Para todas las personas, incluidos los menores de edad:
  - Para el aprovisionamiento de servicios de medición, análisis y de cualquier otro tipo para empresas, en los que somos responsables del tratamiento de los datos en calidad de controladores. Nuestros intereses legítimos a la hora de llevar a cabo el tratamiento de datos correspondiente se basan en los siguientes fundamentos:
    - Proporcionar informes precisos y fiables a nuestros anunciantes, desarrolladores y socios para garantizar la exactitud de los datos facilitados en cuanto a precios y estadísticas de rendimiento, y demostrar el valor que obtienen nuestros socios a través de los productos de las empresas de *Facebook*.
    - En interés de los anunciantes, desarrolladores y socios, ayudarles a comprender a sus clientes y mejorar sus empresas, validar nuestros modelos de precios y evaluar la eficacia de su publicidad y su contenido en internet, dentro y fuera de los productos de las empresas de *Facebook*.
  - Para el envío de comunicaciones de marketing que te hacemos llegar. Nuestros intereses legítimos a la hora de llevar a cabo el tratamiento de datos correspondiente se basan en los siguientes fundamentos:
    - Promocionar los productos de las empresas de *Facebook* y llevar a cabo nuestras tareas de marketing directo.
  - Para la realización de tareas de investigación e innovación en aras del bienestar social. Nuestros intereses legítimos a la hora de llevar a cabo el tratamiento de datos correspondiente se basan en el siguiente fundamento:
    - Divulgar el conocimiento académico y de vanguardia sobre temas de relevancia social para contribuir a mejorar nuestra sociedad y el mundo en el que vivimos.
  - Para compartir información con terceros, incluidas las fuerzas del orden, y responder a requerimientos legales. Nues-

de contenidos y servicios digitales (*Google*[86] y *Apple*[87]); plataforma de música en *streaming* (*Spotify*[88]); plataforma de servicios *cloud* (*Dropbox*[89]).

tros intereses legítimos a la hora de llevar a cabo el tratamiento de datos correspondiente se basan en los siguientes fundamentos:

- Para detectar, impedir y abordar casos de fraude, uso no autorizado de los productos de las empresas de *Facebook,* incumplimiento de nuestras políticas o condiciones, así como otras actividades perjudiciales o ilegales; para protegernos (incluidos nuestros derechos, nuestras propiedades o nuestros Productos), así como para proteger a nuestros usuarios o a otras personas, también como parte de investigaciones o consultas de tipo regulatorio; y para evitar la muerte o daños físicos inminentes.»

[86] *Google* (https://policies.google.com/privacy): «Tratamos tu información para alcanzar nuestros intereses legítimos y los de terceros y, al mismo tiempo, aplicamos medidas de protección adecuadas para garantizar tu privacidad. Esto significa que tratamos tu información con los siguientes objetivos:

- Proporcionar, mantener y mejorar nuestros servicios para satisfacer las necesidades de nuestros usuarios.
- Desarrollar productos y funciones nuevos que sean útiles para nuestros usuarios.
- Saber cómo utilizan los usuarios nuestros servicios para garantizar y mejorar su rendimiento.
- Personalizar nuestros servicios para ofrecerte una mejor experiencia de usuario.
- Promocionar nuestros servicios entre los usuarios. *Google* muestra publicidad, lo que permite que muchos de sus servicios sean gratuitos (en el caso de los anuncios personalizados, pedimos tu consentimiento).
- Detectar, prevenir o solucionar de otra forma fraudes, abusos y problemas de seguridad o técnicos relacionados con nuestros servicios.
- Proteger a *Google*, a nuestros usuarios y al público en general de daños a sus derechos y propiedades o a su seguridad en la medida exigida o permitida por la ley, lo que incluye la revelación de información a autoridades gubernamentales.
- Llevar a cabo investigaciones que mejoren nuestros servicios para los usuarios y beneficien al público en general.
- Cumplir las obligaciones con nuestros *partners*, como desarrolladores y titulares de derechos.
- Responder a reclamaciones legales, incluida la investigación de posibles infracciones de las condiciones de servicio aplicables.»

[87] *Apple* (https://www.apple.com/es/legal/privacy/es/): En este caso, la entidad no especifica la concreta base legal, con carácter general indica: «Podemos procesar tus datos de carácter personal: para los fines descritos en esta Política de Privacidad, con tu consentimiento, para cumplir con un mandato legal al que esté sujeto *Apple*, para cumplir un contrato del que tú formas parte, para proteger tus intereses vitales, o si consideramos que es necesario para los intereses legítimos de *Apple* o un tercero al que haya que revelar información. Si tienes preguntas sobre esta base legal, puedes contactar con el Delegado de Protección de Datos europeo.»

Cabe deducir, aunque no se recoge expresamente, que el interés legítimo está presente en las siguientes finalidades:

- «Los datos de carácter personal que recogemos nos permiten mantenerte informado acerca de los productos más recientes de *Apple,* las actualizaciones de software disponibles y los próximos eventos. Si no deseas formar parte de la lista de distribución, puedes darte de baja en cualquier momento actualizando tus preferencias.»
- «Asimismo, utilizamos los datos de carácter personal como ayuda para crear, desarrollar, gestionar, entregar y mejorar nuestros productos, servicios, contenidos y anuncios publicitarios, y con el propósito de evitar pérdidas y fraudes. Puede que también usemos tu información personal con motivos de seguridad de red y cuenta como, por ejemplo, para proteger nuestros servicios para el beneficio de todos nuestros usuarios y la evaluación o revisión previa de contenidos cargaros cargados para detectar posibles contenidos ilegales, incluidos los materiales de explotación sexual infantil. Si utilizamos tus datos con el fin de luchar contra el fraude, será debido a una conducta determinada detectada en una transacción online con *Apple*. Limitamos el uso de los datos para luchar contra el fraude a los casos estrictamente necesarios y dentro de nuestros intereses legítimos de proteger a nuestros clientes y servicios. En ciertas transacciones online también es posible que validemos la información que nos hayas proporcionado mediante nuestras fuentes de acceso público.»

[88] *Spotify* (https://www.spotify.com/es/legal/privacy-policy/): La plataforma recoge simultáneamente como bases legitimadoras la ejecución de un contrato (art. 6.1.b RGPD) y el interés legítimo (art. 6.1.f RGPD) para las siguientes finalidades:

- «Proporcionar, personalizar y mejorar su experiencia con el Servicio *Spotify* y otros servicios y productos proporcionados por *Spotify*, por ejemplo, proporcionando contenido personalizado, a medida o localizado, recomendaciones, funciones y publicidad dentro o fuera del Servicio *Spotify* (incluidos para productos y servicios de terceros).
- Comprender cómo acceder y utilizar el Servicio *Spotify* para asegurar la funcionalidad técnica del Servicio *Spotify*, desarrollar nuevos productos y servicios, y analizar su uso del Servicio *Spotify*, incluyendo su interacción con las aplicaciones, publicidad, productos y servicios que están disponibles, vinculados u ofrecidos a través del Servicio *Spotify.*
- Comunicarse con usted para fines relacionados con el Servicio *Spotify*.
- Procesar su pago para prevenir o detectar fraudes, incluyendo pagos fraudulentos y uso fraudulento del Servicio *Spotify*.»

Utiliza como bases legitimadoras tanto el consentimiento (art. 6.1.a RGPD) como el interés legítimo (art. 6.1.f RGPD) para la siguiente finalidad: «Comunicarse con usted, ya sea directamente o a través de uno de nuestros socios, para: marketing, investigación, participación en encuestas, concursos, sorteos y promociones, a través de mensajes de correo electrónico, notificaciones u otros mensajes, conforme a los permisos que puede habernos comunicado (p. ej., a través de la página Configuración de cuenta).»

[89] *Dropbox* (https://help.dropbox.com/es-es/accounts-billing/security/privacy-policy-faq.): «*Dropbox* procesa tus datos (1) para proporcionarte los Servicios de *Dropbox* conforme a nuestro contrato contigo; (2) en cumplimiento de sus intereses legítimos en relación con el funcionamiento de nuestros Servicios y negocio; y (3) con tu consentimiento. Entre los ejemplos de cómo procesa *Dropbox* tus datos en cumplimiento de sus intereses legítimos en lo relativo al funcionamiento de nuestros Servicios y negocio se incluyen los siguientes:

4. Datos de categoría especial (art. 9 RGPD)

44. ¿*Quid* cuando el consumidor facilita o se compromete a facilitar el tratamiento de datos de categoría especial para finalidades diferentes al suministro de contenidos o servicios digitales?, ¿resulta alterada la base de legitimación en los contratos en los que el consumidor facilita datos biométricos, genéticos, de salud, ideología…? Pensemos en contenidos o servicios digitales que solicitan datos de las siguientes categorías:

i. Datos de geolocalización o ubicación, que pueden revelar información especialmente sensible sobre ideología, creencias religiosas, condiciones de salud y permitir la elaboración de perfiles o de decisiones automatizadas[90].
ii. Grabaciones de asistentes virtuales de voz (Siri, *Google Home*, Alexa[91]…) o captación de sonidos realizada por aplicaciones móviles (aplicación móvil appLALIGA) puede igualmente revelar datos de esta índole e impactar en otros ámbitos de la esfera privada de las personas.
iii. Datos biométricos, como los que pueden extraerse a partir de fotografías o videos facilitados por los usuarios, por la ultimamente viral aplicación rusa *FaceApp*, que supuestamente imagina el envejecimiento, o la china *Zao*, que superpone la imagen de la cara de una persona a la de un famoso en una serie o película.
iv. Datos de salud, como el ritmo cardiaco registrado por dispositivos de entrenamiento o seguimiento de la salud.

45. En tales supuestos, debe, además, cumplirse una de las circunstancias previstas en el artículo 9.2 RGPD que exceptúan la prohibición general de tratamiento de estos datos de categoría especial contenida en el número primero del precepto, a saber: consentimiento explícito del interesado; cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del Derecho laboral y de la seguridad y protección social; protección de intereses vitales del interesado o de otra persona física, actividades legítimas y con las debidas garantías realizadas por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre

– Comprender cómo utilizas nuestros Servicios y mejorarlos.
– Promover los Servicios de Dropbox más relevantes para tus intereses.
– nvestigar y evitar que se produzcan incidencias de seguridad, infracciones en los Servicios de Dropbox o abusos a usuarios de *Dropbox*.»

[90] Junto con aplicaciones propiamente de localización (*Google Maps*, Mapas, *Waze*…) numerosas utilizan datos de est tipo: deportivas como *Strava, Movescount*…; de transporte como *Uber, Cabify*…; para tarjetas y billetes de avión y tren como *Passbook* y *Wallet;* redes sociales como *Facebook, Twitter, Instagram, YouTube, WhatsApp*…; aplicaciones de *Google*, incluidas *Chrome*, Fotos, Música, Películas, *Store*…; la cámara y la galería; el reloj y el calendario

[91] Según la política de privacidad de *Apple* (https://www.apple.com/es/legal/privacy/es/): «Siri está diseñado para que aprenda todo lo posible sin conexión, directamente en tu dispositivo. Las búsquedas y peticiones no se asocian a tu ID de *Apple*, sino que se vinculan a un identificador aleatorio compuesto por una larga secuencia de letras y números». Accesible en https://www.apple.com/es/legal/privacy/es/. Por su parte, *Google* advierte: «*Google Home* escucha pequeños fragmentos (unos segundos) para detectar la palabra activa. Si no la encuentra, la información permanece en tu dispositivo y los fragmentos se eliminan. Cuando *Google Home* detecta que has escrito "*Ok Google*" u "*Hey Google*" o que has pulsado la parte superior del dispositivo *Google Home*, los LED del dispositivo se iluminan para indicarte que *Google Home* registra lo que dices y envía esa grabación (incluida la grabación de la palabra activa de pocos segundos) a *Googl*e para satisfacer tu solicitud. Puedes eliminar estas grabaciones a través de Mi actividad en cualquier momento. Si utilizas tu voz para interactuar con el Asistente, es posible que usemos el texto de esas interacciones para obtener información sobre tus intereses y personalizar los anuncios. Puedes revisar tus ajustes de *Google* siempre que quieras para controlar los anuncios que ves e incluso para inhabilitar la personalización de anuncios por completo». Accesible en https://support.google.com/googlenest/topic/7173611?hl=es. Según *Amazon*: «Cuando le hablas a Alexa, una grabación de lo que le has preguntado se envía a los servidores de *Amazon* para que nuestros sistemas de reconocimiento de voz y comprensión del lenguaje natural puedan procesar y responder a tu petición. Asociamos tus solicitudes con tu cuenta *Amazon* para que puedas acceder a otros servicios de Amazon (por ejemplo, para que puedas pedirle a Alexa que te lea tus libros *Kindle*) y ofrecerte una experiencia más personalizada (por ejemplo, hacer un seguimiento de las canciones que hayas escuchado ayudará a Alexa a elegir qué canciones reproducir cuando le digas "Alexa, pon música")». Accesible en https://www.amazon.es/gp/help/customer/display.html/?nodeId=GA7E98TJFEJLYSFR.

que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados; datos personales que el interesado ha hecho manifiestamente públicos; formulación, ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros; fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; razones de interés público en el ámbito de la salud pública; y fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Eso sí no se debe perder de vista que el hecho de que sea aplicable una circunstancia del artículo 9.2 RGPD no elimina que el responsable deba de asegurarse de que concurre al mismo tiempo una base de tratamiento general del art**ículo** 6. Las causas legitimadoras del artículo 6 y las circunstancias del artículo 9 se aplican conjuntamente, cada una en su propio ámbito[92].

46. En la mayor parte de los contratos de suministro de contenidos y servicios digitales, las circunstancias (entre las que no figura ni la necesidad del tratamiento para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales *ex* artículo 6.1.b, ni para la satisfacción del interés legítimo del responsable o de un tercero *ex* artículo 6.1.f) que podrán justificar que el consumidor pueda comprometerse a facilitar datos de categoría especial del artículo 9 RGPD serán el consentimiento, un consentimiento aún más reforzado al que se le añade la condición de que sea explícito, o el tratarse de datos que se han hecho manifiestamente públicos[93]. No obstante, el tratamiento de categorías especiales de datos personales en virtud del consentimiento explícito no es una base aplicable en todo caso, dado el el RGPD permite que «el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado» (art. 9.2.a RGPD)[94]. Precisamente, esta habilitación ha permitido que la LOPDGDD establezca que «a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal –no accesoria- sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico» (art. 9.1 LOPDGDD). Por tanto, el consentimiento explícito sólo puede legitimar los tratamientos de algunas categorías especiales como datos de salud, datos genéticos y datos biométricos. Conviene, pues, a la vista de estas especialidades nacionales, llamar la atención sobre clausulados de empresas que operan en todo el ámbito europeo y que, como es el caso de *Facebook* e *Instagram*[95], justifican en el consentimiento: el «tratamiento de datos de categorías especiales (como creencias religiosas, ideologías políticas, qué personas te interesan o información sobre tu salud, si compartes estos datos en los acontecimientos importantes o los distintos campos de tu perfil de *Facebook*), de modo que podamos compartirlos con quien determines y personalizar tu contenido»; también *Google* específica que solicitará el consentimiento explícito para

[92] Así lo señala expresamente el GT29 en sus *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, de 3 de octubre de 2017, revisadas el 6 de febrero de 2018, pág. 16: «C. Artículo 9 - Categorías especiales de datos: "Los responsables del tratamiento solo pueden tratar datos personales de categoría especial si se cumplen una de las condiciones previstas en el artículo 9, apartado 2, así como una condición del artículo 6. Esto incluye datos de categoría especial derivados o inferidos de la actividad de la elaboración de perfiles. Esta actividad puede crear datos de categoría especial por inferencia a partir de datos que no pertenecen a una categoría especial por derecho propio pero que entran en ella al combinarse con otros datos. Por ejemplo, es posible inferir el estado de salud de una persona a partir de los registros de su compra en combinación con datos sobre la calidad y el contenido energético de los alimentos. Pueden hallarse correlaciones que indiquen algo sobre la salud, las convicciones políticas, las creencias religiosas o la orientación sexual de las personas, como demuestra el siguiente ejemplo: Ejemplo: Un estudio combinó los «me gusta» de *Facebook* con información limitada procedente de encuestas y halló que los investigadores predijeron con exactitud la orientación sexual de un usuario varón en el 88 % de los casos; el origen étnico de un usuario en el 95 % de los casos; y si un usuario era cristiano o musulmán en el 82 % de los casos. »

[93] Vid. J. A. Messía de la Cerda Ballesteros, "El tratamiento de los datos personales que el interesado hubiese hecho manifiestamente públicos. Especial atención a las Redes Sociales", *Actualidad Civil*, Nº 5, 2018.

[94] Como también es potestad de los Estados miembros mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud (art. 9.4 RGPD).

[95] Accesible en https://www.facebook.com/about/privacy/legal_basesel fecha de sobre cookies de 18web citados en este trabajo se ha realizado el 15 de diciembre de 2019.forme sobre cookies de 18.

compartir cualquier información personal sensible, aclarando que «esta información personal se incluye en una categoría especial por estar relacionada con datos médicos de carácter confidencial, información sobre raza u origen étnico, creencias religiosas, ideología política o sexualidad».

V. Algunas conclusiones

47. La delimitación de la licitud de tratamiento de datos personales en los contratos cubiertos por la DCDig., en lo que el consumidor facilita datos al empresario para su tratamiento *con finalidades distintas al suministro o al cumplimiento de obligaciones legales a cambio de acceder a contenidos o servicios digitales,* plantea enorme complejidad en el actual ecosistema digital, caracterizado por su estandarización y predisposición.

48. Reconocida por la DCDig. la reciprocidad de prestaciones en estos contratos, el tratamiento de tales datos sería lícito por ser necesario para el cumplimiento de las obligaciones asumidas por el consumidor titular de los datos y, en consecuencia, necesario para la ejecución del contrato (art. 6.1.b RGPD). En estos casos, la autorización por el consumidor del tratamiento de sus datos personales se inserta en el propio consentimiento contractual, sin posibilidad de libre revocación conforme al artículo 7.3 RGPD, por lo que el foco de atención debería desplazarse a los intrumentos de protección del consumidor (transparencia, cláusulas abusivas, desistimiento…) conectados con los principios aplicables a cualquier tratamiento de datos conforme al RGPD. No obstante, esta contemplación de la cuestión se opone frontalmente a la interpretación realizada por las instancias y autoridades europeas de protección de datos que reiteramente abogan por una lectura de los términos de "necesidad" y "ejecución contractual" estricta y unilateral, esto es, desde óptica de la adecuación del tratamiento de los datos al cumplimiento de las prestaciones asumidas por el proveedor de contenidos o servicios digitales.

49. Un entendimiento más acorde con la tradicional visión del derecho a la protección de datos, como poder de control y de disposicion sobre la propia información personal, conduce a legitimar tal injerencia del proveedor en la esfera personal de consumidor sobre la base del consentimiento del propio titular de los datos. Lo que, al margen de la necesidad de distinguir netamente el consentimiento contractual y el consentimiento para el tratamiento de datos, así como las implicaciones contractuales que han quedado expuestas, la cuestión a responder, dado el estandar más exigente del consentimiento derivado del RGPD, es si realmente, en el escenario de la contratación de prestaciones digitales, al aceptar términos predispuestos nos encontramos ante consentimientos al tratamiento de los propios datos personales derivados de una verdadera y adecuada manifestación de voluntad por la que el consumidor realmente ejerza el control de su información personal y cuenta con libertad de elección[96]. El consentimiento implica control, libertad por parte del titular, si este no tiene realmente libertad de elección**,** su consentimiento no será libre, ni válido. Además, en estos supuestos basados en términos y condiciones generales impuestas unilateralmente, con frecuencia existe confusión entre:

a. Aceptar que se ha recibido la información preceptiva en protección de datos ("*accountability*").
b. Autorizar el tratamiento de datos personales ("consentimiento" *ex* 6.1.a RGPD)[97].
c. Consentir el vínculo contractual.

[96] Vid. J. López Calvo, "Las crecientes exigencias del consentimiento y el control institucional del clausulado en protección de datos", *Diario La Ley*, Nº 10, Sección Ciberderecho, 11 de Septiembre de 2017.

[97] Ilustrativo en este sentido pueden ser los mecanismos de obtención del consentimiento reseñados en la *Guía AEPD sobre cookies*, publicada en noviembre 2019 (accesible en https://www.aepd.es/media/guias/guia-cookies.pdf). Entre otros, la *Guía* recoge los siguientes: a) la obtención del consentimiento al solicitar el alta en un servicio, siempre que este consentimiento esté separado y no se agrupe con la aceptación de los términos y condiciones de uso de la página web, de su política de privacidad o de las condiciones generales del servicio; b) Durante el proceso de configuración del funcionamiento de la página web o aplicación, en el momento de la elección o especificación por parte del usuario de las características, quedando el consentimiento integrado en la elección del usuario; c) Bajo determinadas condiciones, a través de plataformas de gestión del consentimiento (consent management platform o CMP); d) Antes del momento en que se vaya a descargar un servicio o aplicación ofrecido,

50. El recurso al interés legítimo como base legitimadora de determinadas finalidades distintas al suministro de contenidos y servicios digitales es frecuente en los clausulados y políticas de privacidad de los proveedores de prestaciones digitales, no obstante el área de riesgo en el empleo de esta causa de licitud es elevada cuando no resulta claro, como suele suceder, cuáles son los intereses legítimos que hipotéticamente pueden legitimar el tratamiento de sus datos o es cuestionable el proceso de ponderación entre el interés legítimo del responsable o de terceros y los intereses, derechos y libertades de los consumidores.

51. El análisis de los clausulados de privacidad de las principales plataformas tecnológicas pone de manifiesto que el tratamiento de datos personales a cambio del acceso a contenidos y servicios digitales sigue las directrices interpretativas de las autoridades europeas en cuanto a basar en la ejecución contractual principalmente el tratamiento de datos acorde a la prestación del servicio ofrecido (otra cuestión a valorar sería la observancia del principio de minimización, en cuanto a la adecuación, pertinencia y limitación a los datos necesarios), recurriendo, principalmente, al consentimiento y al interés legítimo del responsable o de terceros para finalidades diferentes al propio suministro. No obstante, de una comparativa de los clausulados utilizados en este trabajo pueden extraerse varias conclusiones:

— El uso de los datos para idéntica finalidad es soportado por bases legitimadoras no coincidentes entre las diferentes plataformas y operadores;
— Se recurre cumulativa e indistintamente por un mismo responsable a varias bases de legitimación del tratamiento de datos para justificar una misma finalidad;
— No siempre resulta evidente que la obtención del consentimiento se verifique separadamente para cada tratamiento basado en el mismo, así como por cada uno de los responsables que vayan a tratar autónomamente los datos personales así recogidos, dado que el permitir que terceros traten la información personal implica corresponsabilidad (STJUE de 29 de julio de 2019, C40/17, Fashion ID)[98];
— La obtención del servicio queda en ocasiones supeditada a la autorización para el tratamiento de datos personales;
— Cabe dudar, en ocasiones, de la prevalencia del interés legítimo del responsable o de terceros sobre los intereses, derechos y libertades de los consumidores, especialmente tratándose de menores de edad.

52. Pero, probablemente, la principal conclusión que puede extraerse de este análisis es que la concreción de la base jurídica que, conforme a las previsiones del artículo 6 RGPD, da soporte a los tratamientos derivados de contratos a los que resulta aplicable la DCDig., particularmente de aquellos datos facilitados para ser tratados con finalidades distintas al suministro de contenidos o servicios digi-

siempre que no se condiciones el acceso a la aplicación o servicio al consentimiento… No obstante, resulta llamativa una precisión que contiene la *Guía* respecto de las *cookies wall,* es decir, aquellas que impiden el acceso a un contenido a menos que se acepte. La AEPD considera que son lícitas, salvo en el caso de que «el usuario desee ejercitar un derecho que le está legalmente reconocido (por ejemplo, la baja en un servicio telefónico, de acceso a Internet o de otro tipo) y la aplicación o servicio es el único medio facilitado». Mucho más acertado resulta, a mi modo de ver, el criterio de la Autoridad de control francesa, la Commission Nationale de l'Informatique et des Libertés (CNIL), en su informe sobre cookies de 18 de julio de 2019: «la pratique qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à être suivi (*cookie walls*) n'est pas conforme au RGPD». Vid. *Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs*), accesible en https://www.legifrance.gouv.fr/.

[98] Resuelve una cuestión prejudicial plateada a raíz del hecho de que *Fashion ID*, empresa de comercio electrónico dedicada a la venta de prendas de vestir, tenga insertado en su sitio de Internet el botón "me gusta" de *Facebook*, de modo que cuando un visitante consulta el sitio de *Fashion ID*, se transmiten a *Facebook Ireland* datos personales de ese visitante, sin que sea consciente de ello y con independencia de si es miembro de la red social *Facebook* o de si clicó en el botón «me gusta» de *Facebook*, concluyendo el TJUE que «el administrador de un sitio de Internet, como *Fashion ID*, que inserta en dicho sitio un módulo social que permite que el navegador del visitante de ese sitio solicite contenidos del proveedor de dicho módulo y transmita para ello a ese proveedor datos personales del visitante puede ser considerado responsable del tratamiento, en el sentido del artículo 2, letra d), de la Directiva 95/46. Sin embargo, esa responsabilidad se limita a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente, a saber, la recogida y la comunicación por transmisión de datos en cuestión».

tales o al cumplimiento de requisitos legales, no es única. La variedad de finalidades para la que pueden ser utilizados los datos personales que el consumidor facilita o se compromete a facilitar al proveedor a cambio de acceder a contenidos y servicios digitales comporta que, a la vista de la interpretación dada por las instituciones europeas, contraria a equiparar tratamiento necesario para la ejecución del contrato *ex* artículo 6.1.b RGPD y tratamiento de datos ofrecidos, a modo de contraprestación, para ser tratados con finalidades distintas al suministro, deba concretarse la licitud del tratamiento de los datos personales del consumidor en atención a cada una de las finalidades pretendidas por el proveedor, pudiendo concurrir una pluralidad de bases legitimadoras que den soporte a un solo contrato amparado por la DCDig. La expresión "*datos facilitados por el consumidor para su tratamiento con finalidades distintas al suministro o al cumplimiento de obligaciones",* que permite incardinar el contrato celebrado en el marco protector de la DCDig., debe entenderse como una expresión genérica que puede aglutinar un conjunto mayor o menor de bases de licitud en función de cuales sean las concretas finalidades. Su correcta determinación por el proveedor-responsable del tratamiento y su adecuación a la finalidad del tratamiento conforman, junto con otras, una de las principales medidas de cumplimiento normativo que derivan del principio de responsabilidad proactiva eje de todo el sistema de protección de datos articulado por el RGPD.