

LA CONTRAPRESTACIÓN EN FORMA DE DATOS
PERSONALES: EL NUEVO PARADIGMA EN LA ERA DIGITAL

*THE COUNTER-PERFORMANCE IN THE FORM OF PERSONAL
DATA: THE NEW PARADIGM IN THE DIGITAL AGE*

Actualidad Jurídica Iberoamericana N° 22, enero 2025, ISSN: 2386-4567, pp. 1122-1185

Álvaro BUENO
BIOT

ARTÍCULO RECIBIDO: 13 de noviembre 2024

ARTÍCULO APROBADO: 7 de enero de 2025

RESUMEN: El presente trabajo examina la función de los datos personales como contraprestación en el mercado digital. En concreto, defiende su uso como contraprestación en los contratos de suministro de contenidos y servicios digitales y analiza el consentimiento como base legítima para el tratamiento de los mismos. También se abordan las distintas bases jurídicas que pueden legitimar su tratamiento, especialmente, cuando son utilizados con fines comerciales, así como los distintos problemas que se derivan de la interacción entre la normativa de protección de datos y la normativa de consumo.

PALABRAS CLAVE: Datos personales; contraprestación; contenidos y servicios digitales; mercado digital; Directiva 2019/770; TRLGDCU; consumidores y usuarios.

ABSTRACT: *This paper examines the role of personal data as consideration in the digital market. In particular, the paper defends the use of personal data as consideration in contracts for the supply of digital content and digital services, and analyses consent as a legitimate basis for the processing of personal data. The paper also addresses the different legal bases that can legitimise such processing, especially when personal data are used for commercial purposes, as well as the different problems arising from the interaction between data protection and consumer law.*

KEY WORDS: *Personal data; consideration; digital content and digital services; digital market; Directive 2019/770; TRLGDCU; consumers and users.*

SUMARIO.- I. CONSIDERACIONES GENERALES SOBRE LA IMPORTANCIA DE LOS DATOS PERSONALES DEL CONSUMIDOR EN EL MERCADO DIGITAL.- II. EN DEFENSA DEL RECONOCIMIENTO DE LOS DATOS PERSONALES COMO CONTRAPRESTACIÓN.- III. MARCO JURÍDICO DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ÁMBITO DE LOS CONTENIDOS Y SERVICIOS DIGITALES.- I. Sobre el alcance del derecho a la protección de los datos personales.- 2. Normativa aplicable a la protección de los datos personales.- IV. EL CONSENTIMIENTO COMO BASE LEGÍTIMA PARA EL TRATAMIENTO DE DATOS PERSONALES.- V. LOS REQUISITOS PARA OBTENER UN CONSENTIMIENTO VÁLIDO.- 1. Consentimiento libre.- 2. Consentimiento específico.- 3. Consentimiento informado.- 4. Consentimiento inequívoco.- VI. ¿CUÁNDO Y CÓMO SE TIENEN QUE CEDER LOS DATOS PERSONALES POR PARTE DEL CONSUMIDOR?.- VII. SUPUESTOS EN QUE LOS DATOS PERSONALES NO CONSTITUYEN LA CONTRAPRESTACIÓN DEL CONTRATO.- VIII. LAS BASES JURÍDICAS QUE PUEDEN LEGITIMAR EL TRATAMIENTO DE LOS DATOS PERSONALES CUANDO ESTOS SE UTILIZAN PARA FINES COMERCIALES.- 1. Tratamiento basado en la necesidad para la ejecución del contrato ex art. 6.1, letra b) RGPD.- 2. Tratamiento basado en el interés legítimo ex art. 6.1, letra f) RGPD.- 3. Consentimiento del consumidor ex art. 6.1, letra a) RGPD.- IX. PROBLEMAS JURÍDICOS QUE SE PLANTEAN EN RELACIÓN CON EL RGPD.- 1. La contradicción entre la obligación de ceder los datos personales como contraprestación y el derecho a revocar el consentimiento.- 2. La incidencia en el contrato de un consentimiento inválido al tratamiento de datos personales.- 3. Sobre las limitaciones previstas en los arts. 7.4 RGPD y 6.3 LOPDGD.

I. CONSIDERACIONES GENERALES SOBRE LA IMPORTANCIA DE LOS DATOS PERSONALES DEL CONSUMIDOR EN EL MERCADO DIGITAL

Con la creciente evolución de las nuevas tecnologías se han apreciado cambios en la forma de contratar, tanto para consumidores como para empresarios. En este sentido, es frecuente que los contenidos o servicios digitales se suministren, no solo cuando el consumidor paga un precio, sino también cuando facilita datos personales, ya que cada vez es más común que los proveedores de contenidos y servicios digitales no cobren en dinero por la prestación, sino que exijan a cambio de ésta una contraprestación no dineraria, como pueden ser los datos personales (o no) del usuario. Estos modelos de negocio son cada vez más habituales y aparecen de diferentes formas en una parte considerable del mercado¹. De esta forma, las referidas compañías proceden al almacenamiento, tratamiento y transferencia de

¹ Las compañías se dedican a obtener los datos personales de los usuarios, que los ceden, a cambio del uso de una App, de la utilización de los diferentes servicios de las redes sociales o de la activación de la geolocalización del *Smartphone*, entre otros. Sin embargo, como señalan MARTÍNEZ VELENCOSO, L.M. y SANCHO LÓPEZ, M.: "El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?", *InDret: Revista para el Análisis del Derecho*, núm.1, 2018, p.24, los datos de cada persona no son en sí los más relevantes, sino que lo más valioso es la obtención de información sobre la totalidad de nuestra actividad online, lo cual permite rastrear nuestras reacciones, pautas y preferencias y catalogar así nuestro patrón de comportamiento en base a una visión comercial. Así, los datos individualmente considerados van cobrando relevancia en la medida en que se cruzan con otros datos y permiten una reconstrucción de la personalidad online capaz de predecir nuestros pasos o intereses en la vida real.

• Álvaro Bueno Biot

Profesor Ayudante Doctor de Derecho Civil en la Universidad de Valencia. Doctor en Derecho por las Universidades de Valencia y de Bolonia. Correo electrónico: alvaro.bueno@uv.es

estos datos que, estructurados a gran escala, constituyen información de gran valor para otros sujetos que están dispuestos a pagar enormes cantidades de dinero a cambio de ellos. Es lo que se conoce como “Big Data”, el cual consiste en el análisis masivo de datos². En tal sentido, se tratan grandes cantidades de datos que, conjuntamente organizados y analizados³, producen una información muy valiosa, que resulta de gran utilidad de cara a tomar mejores decisiones y movimientos en negocios estratégicos⁴.

Es importante, en este sentido, destacar el papel que ostenta el tratamiento de datos personales en el mercado. Su relevancia económica se puede deducir de los distintos fines para los que son destinados, como la reducción de costes de investigación de los productos y transacciones, su empleo con propósitos de investigación científica –como la inteligencia artificial- y, entre otras utilidades, destaca su uso para la mejora de los resultados de las campañas de publicidad, siendo esencial para la denominada *targeted advertisement* o publicidad dirigida⁵. Es por ello que, en la economía digital, muchos modelos de negocio, tales como los servicios de redes sociales más importantes, los buscadores de internet, determinados servicios de comunicación y numerosos suministradores de contenidos digitales, dependen en menor o mayor medida del tratamiento de

- 2 ONTIVEROS BAEZA, E.: “El *big data* y su importancia en el mundo digital”, en AA.VV.: *Economía de los datos. Riqueza 4.0* (dir. por E. ONTIVEROS BAEZA), Fundación Telefónica – Ariel, S.A., 2017, p. 35, señala que el Big Data hace referencia a “la aparición y el aprovechamiento de grandes volúmenes de datos que, si bien algunos de ellos existían antes, nunca hasta ahora se habían contemplado como una fuente de valor para las empresas, de transparencia para las Administraciones públicas o de mejor autogestión para todos los ciudadanos en su día a día”.
- 3 Estos datos que conforman lo que se denomina el *Big data* se caracterizan, como señala NAVAS NAVARRO, S.: “El internet de las cosas”, en AA.VV. *Mercado digital: principios y reglas jurídicas* (dir. por S. NAVAS NAVARRO y S. CAMACHO CLAVIJO), Tirant lo Blanch, Valencia, 2016, p. 24, por su volumen, velocidad, volubilidad, valor, variedad, visualización y veracidad. En el mismo sentido, STAUDENMAYER, D.: “Comentario al art. 3 Directiva (UE) 2019/770”, en AA.VV.: *EU Digital Law. Article-by-Article Commentary* (dir. por R. SCHULZE y D. STAUDENMAYER), Nomos Verlagsgesellschaft, Baden-Baden (Munich), 2020, p. 69, señala que los macrodatos a menudo se caracterizan por hacer referencia a las 3 V's: gran volumen, gran velocidad y gran variedad.
- 4 Para un análisis más exhaustivo sobre el modelo de negocio consistente en el tratamiento de datos personales y los riesgos que ello conlleva, vid., FRAMINÁN SANTAS, J.: “Big data, consentimiento para tratar datos personales y Derecho de Defensa de la competencia”, *Revista de Derecho Mercantil*, núm. 310, 2018, pp. 1-6.
- 5 DOMÍNGUEZ YAMASAKI, M. I.: “El tratamiento de datos personales como prestación contractual. Gratuidad de contenidos y servicios digitales a elección del usuario”, *Revista de derecho privado*, núm. 4, 2020, p. 98. En el mismo sentido, HOOFNAGLE, C.J. y WHITTINGTON, J.: “Free: Accounting for the Costs of the Internet's Most Popular Price”, *UCLA Law Review*, vol. 61, rev. 606, 2014, p. 626, apuntan que para algunas empresas, la recogida y monetización de datos sobre los consumidores a cambio de servicios supuestamente gratuitos es la principal propuesta de negocio. Estos modelos de negocio demuestran hasta qué punto las empresas valoran, como cualquier otro activo, la información personal que recopilan sobre cada consumidor, especialmente cuando el consumidor es un beneficiario gratuito. Sin embargo, CASTILLO PARRILLA, J.A.: “Economía digital y datos entendidos como bienes”, en AA.VV.: *El mercado digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, S.A., Madrid, 2019, p. 286, matiza que “el foco sobre el mercado de datos no debe proyectarse exclusivamente a partir de los datos como parte integrante de un conjunto estructurado potencialmente útil en un momento posterior a través de técnicas de tratamiento y análisis de datos, pues de este modo no se estaría observando en su conjunto el mercado de datos en la medida en que no se observa en su conjunto el proceso productivo de los datos. Si aceptamos que los datos son productos (...) y que desempeñan una función económica en tanto que forman parte de un mercado, debemos analizarlos desde el paradigma de la cadena de producción o, dicho de otro modo, observar su comportamiento en el mercado (el de los datos) desde el inicio hasta el final del proceso productivo”.

los datos personales de los usuarios⁶. De ahí que los datos personales se hayan convertido en un activo negociable⁷ y, en consecuencia, se pueda afirmar que son “la nueva moneda del mundo digital”⁸. De esta forma, aunque no haya contraprestación dineraria en este tipo de contratos, el proveedor exige una serie de datos que pueden ser de gran valor para quien los trate y, por ende, el hecho de que el proveedor no cobre en dinero por la prestación que ofrece no significa que este contrato deba ser considerado como gratuito, ya que dicha gratuidad es solo aparente, pues, en realidad, existe una contraprestación que consiste en la autorización que otorga el usuario al tratamiento de sus datos personales⁹.

Es cierto que la solución ideal pasa por realizar una aproximación al valor económico que puedan tener los datos personales cedidos a modo de contraprestación con la finalidad de objetivar ese “precio”¹⁰. Sin embargo, el problema que se plantea es la difícil valoración de los datos personales. No se puede negar que, a través de su empleo (por ej. de las redes sociales), el usuario/consumidor genera datos personales que son una fuente económica valiosa para los proveedores de dichos servicios¹¹. Pero, si bien es cierto que existen algunos estudios en los que se proponen algunas vías para determinar el valor de los mismos¹², se plantean numerosas dificultades a la hora de arrojar un valor

- 6 VERSACI, G.: “Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection”, *European Review of Contract Law*, vol. 14, núm.4, 2018, p. 376.
- 7 STAUDENMAYER, D.: “Comentario al art. 3 Directiva (UE) 2019/770”, cit., p. 69.
- 8 LANGHANGE, C. y SCHMIDT-KESSEL, M.: “Consumer Data as Considetarion”, *Journal of European Consumer and Market Law*, vol. 4, núm. 6, 2015, p. 218.
- 9 SANTOS MORÓN, M.J.: “Consumidor y nuevas tecnologías: privacidad y protección de datos”, en AA.VV.: *Derecho de consumo: visión normativa y jurisprudencial* (coord. por M.J. SANTOS MORÓN y M.N. MATO PACÍN), Madrid, 2022, p. 304. En este sentido, como señala CÁMARA LAPUENTE, S.: “Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad”, en AA.VV. *El mercado digital en la Unión Europea* (dir. por. P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, Madrid, 2019, p. 204, podría considerarse como práctica comercial desleal aquella en la que el proveedor del contenido o servicio digital destaca la gratuidad absoluta del servicio cuando puede que existan cargos ocultos en forma de recolección de datos con su valor que harían engañosa la afirmación (Cfr. Art. 22.5 Ley de Competencia Desleal). Vid., en este mismo sentido, FRISANI, C. y VALLI, M.: “Consumatori di beni con elementi digitali e di contenuti e servizi digitali e pratiche commerciali sleali”, en AA.VV.: *I diritti dei consumatori digitali* (dir. por. R. TORINO), Pacini Giuridica, Pisa, 2023, p. 191, quienes manifiestan que constituye una práctica comercial desleal el hecho de que la empresa promueva la percepción de que los contenidos o servicios digitales se prestan de forma gratuita, toda vez que exige al consumidor que proporcione información personal con la finalidad de que sea tratada para fines comerciales. En la misma línea, vid., DE FRANCESCHI, “Personal Data as Counter-Performance”, en SENIGAGLIA, IRTI y BERNES (coords.) *Privacy and Data Protection in Software Services*, Signapur, 2022, p. 67.
- 10 ROSELLÓ RUBERT, F.M.: “La propuesta de Directiva sobre suministro de contenidos digitales y la protección del consumidor de servicios digitales no retribuidos monetariamente”, en AA.VV.: *El mercado Digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, Madrid, 2019, p. 279.
- 11 ARROYO VENDRELL, T. y SCHULZE, R.: “Contratos de contenidos digitales: Introducción”, en AA.VV.: *Verträge über digitale Inhalte und digitale Dienstleistungen* (coord. por J. KINDL, T. ARROYO VENDRELL y B. GSELL), Nomos Verlagsgesellschaft, Baden-Baden (Alemania), 2018, p.15.
- 12 Vid., en este sentido, OECD, “Exploring the Economics of Personal Data. A survey of methodologies for measuring monetary value”, OECD Digital Economy Papers, 2013, núm. 220, pp. 18 y ss. También, una clara exposición de algunas metodologías que se pueden utilizar para el cálculo del valor de los datos personales puede verse en HERNÁNDEZ MARTÍN, “La privacidad: una mirada desde la economía”, en AA.VV. *En torno a la privacidad y la protección de datos en la sociedad de la información* (coord. por J.P. APARICIO VAQUERO, y A. BATUECAS CALETRÍO), Comares, Granada, 2015, pp. 1-25. En el mismo sentido, se exponen también algunos métodos para el cálculo en NAVAS NAVARRO, S.: “El valor de los datos personales en el mercado”, en

exacto, justo y veraz. Ahora bien, sea cual sea la fórmula que se utilice para su determinación, el cálculo deberá ser transparente y claro, debiendo quedar perfectamente determinado el objeto sobre el que se está asignando un precio y el *modus operandi* que se utiliza para arrojar el valor del objeto del cálculo. En cualquier caso, como señala parte de la doctrina¹³, a pesar de los avances que se van produciendo con respecto a la determinación del valor económico de los datos personales, estos datos del usuario, individualmente considerados, tienen un escaso valor económico, pues los mismos cobran especialmente relevancia cuando, en grandes volúmenes, se cruzan unos con otros a través de lo que ya nos hemos referido como el Big Data¹⁴.

II. EN DEFENSA DEL RECONOCIMIENTO DE LOS DATOS PERSONALES COMO CONTRAPRESTACIÓN.

El legislador, consciente de la realidad social y económica que envuelve este mercado, optó por regular la situación en la que los datos personales aparecen como moneda de cambio de muchos contenidos y servicios digitales, otorgando así una mayor protección a los consumidores y garantizando una mayor seguridad jurídica a los empresarios¹⁵. En este sentido, el art. 59.4 del Texto Refundido de

AA.VV.: *Verträge über digitale Inhalte und digitale Dienstleistungen* (coord. por J. KINDL, T. ARROYO VENDRELL y B. GSELL), Nomos Verlagsgesellschaft, Baden-Baden (Munich), 2018, pp. 111-113; o HACKER, P.: "Regulating the Economic Impact of Data as Counter – Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive", en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSE, R. SCHULZE y D. STAUDENMAYER), Nomos/Hart, Baden-Baden (Munich), 2020, pp. 49-53.

13 *Id.*, entre otros, DOMÍNGUEZ YAMASAKI, M. I.: "El tratamiento de datos personales", cit., p. 99, MARTÍNEZ VELENCOSO, L.M. y SANCHO LÓPEZ, M.: "El nuevo concepto de onerosidad", cit., p. 24; y GONZÁLEZ HERNÁNDEZ, R.: "La protección del consumidor en la contratación digital", *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, p. 1247.

14 Como señala NAVAS NAVARRO, S.: "El internet de las cosas", cit., pp. 27-32, uno de los rasgos característicos de los "big data" es su variedad o heterogeneidad. En este sentido, nos parece interesante traer a colación la distinción que realiza entre lo que denomina "datos-materia prima" y "datos-conocimiento" para una mejor comprensión de por qué los datos personales del consumidor o usuario individualmente considerados tienen un escaso valor. Así, los "datos-materia prima" son aquellos recogidos, en gran parte mediante sistemas informáticos, pero que todavía no han sido tratados, manipulados o cruzados con otros datos. Pueden calificarse como datos de "bajo nivel". En cambio, los "datos-conocimiento" son aquellos que se generan como consecuencia del tratamiento por algoritmos matemáticos de los "datos-materia prima", lo que da lugar a información de gran valor que se puede utilizar para diversas finalidades. Se pueden calificar como datos de "alto nivel". De ahí que los "datos-materia prima" que son los que cede el consumidor o usuario como contraprestación, en sí mismos considerados, tienen una escasa valía, pues realmente lo que constituye una información valiosa son los "datos-conocimiento" que se obtienen del tratamiento y combinación de los "datos-materia prima" a través de los diferentes algoritmos propiedad de cada empresa y protegidos por una doble vía: como "obra original" (art. 10 de la Ley de Propiedad Intelectual) o como derecho *sui generis* del fabricante (arts. 133 y ss de la Ley de Propiedad Intelectual). En un sentido similar se expresa TRIPODI, E.M.: "Consumi digitali e dati personali", en AA.VV.: *I diritti dei consumatori digitali* (dir. por R. TORINO, Pacini Giuridica, Pisa, 2023, p. 277, quien afirma que los datos personales por sí solos valen muy poco o nada, ya que es poco probable que la construcción de una empresa se base en esos datos por sí solos. El valor, en cambio, se compone de todo el procesamiento que se realiza sobre él, precisamente con el fin de conferir el valor, que aumenta a medida que aumenta el número de datos y el consiguiente procesamiento.

15 De esta forma, como señala NAVAS NAVARRO, S.: "El valor de los datos personales", cit., p. 105, lo que se ha hecho a través de los textos normativos no es más que reconocer la existencia "legal" de situaciones en las que el suministro del contenido o servicio digital se ofrecía –erróneamente- de forma "gratuita", y así lo

la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (en adelante, TRLGDCU)¹⁶ reconoce la aplicación del Libro II a “los contratos en virtud de los cuales el empresario suministra o se compromete a suministrar contenidos o servicios digitales al consumidor o usuario y este facilita o se compromete a facilitar datos personales, salvo cuando los datos personales facilitados por el consumidor o usuario sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales objeto de un contrato de compraventa o de servicios 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”¹⁷. Este precepto tiene su origen en el art. 3.1, párrafo 2º de la Directiva 2019/770 (en adelante, DCSD)¹⁸, que es la normativa que reconoce, por primera vez, a los datos personales como contraprestación, lo cual ha supuesto una de las novedades más relevantes y que más interés ha despertado en la doctrina.

consideraba el consumidor, cuando, en realidad, estaba satisfaciendo una contraprestación no pecuniaria en forma de “información personal” o de “datos personales”.

- 16 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 (ELI: <https://www.boe.es/eli/es/rdlg/2007/11/16/1/con>).
- 17 Cabe señalar que la nomenclatura que se le ha dado a este tipo de contratos, es decir, “contrato de suministro de contenidos y servicios digitales”, en realidad, se debe a una deficiente traducción de la versión original de la DCSD al idioma español. La versión original hace referencia a “contracts for the supply of digital content and digital services”, lo que traducido al español sería “contratos para el suministro” y no “contratos de suministro”. Esto puede inducir a confusión, pues no se ha tenido en cuenta que en España el contrato de suministro dispone de una entidad y características propias. De hecho, la DCSD, a diferencia de la Directiva 2011/83, ahora no prohíbe la calificación de los “contratos de suministro de contenidos y servicios digitales” como contratos de venta o de servicios, sino que, más bien al contrario, clarifica que se deja en manos del legislador nacional la calificación de si este tipo de contratos constituyen, por ejemplo, “un contrato de compraventa, de servicios, de alquiler o un contrato atípico”. Sin embargo, el legislador español, con la transposición de la DCSD al TRLGDCU, ha omitido determinar la calificación de este tipo de contratos, a pesar de todas las categorías contractuales que el Cdo. 12 de la DCSD ofrece para que sean los Estados Miembros los que se decanten por alguna de ellas (contrato de compraventa, de servicios, de alquiler o un contrato atípico). Sin embargo, el TRLGDCU dispone únicamente de dos categorías contractuales: “contrato de compraventa o venta” y “contrato de servicios”. Si atendemos a estas dos definiciones reguladas en los arts. 59 bis. 1, letra f) y 59 bis. 1, letra g) TRLGDCU se pueden extraer las siguientes consideraciones: 1) en ambas definiciones desaparece la prestación a la que estaba obligado el consumidor, esto es, que “pague o se comprometa a pagar su precio”. Esto no significa que haya desaparecido la contraprestación dineraria, sino que, más bien al contrario, el legislador ha decidido prescindir de establecer la prestación a la que está obligado el consumidor o usuario, precisamente porque estas instituciones deben abarcar también los contratos de contenidos y servicios digitales en los que la contraprestación consista en la cesión de datos personales por parte del consumidor o usuario; 2) respecto al “contrato de servicios”, se añade al final de la nueva definición que el mismo incluirá también aquellos que tengan “carácter digital”, por lo que es obvio que el legislador ha querido adaptar esta figura a la nueva realidad social, en la cual los contratos de contenidos y servicios digitales también podrán ser encuadrables como contratos de servicios; y 3) por último, cabe precisar que en ninguna de las dos definiciones se hace referencia al suministro de contenidos o servicios digitales. En tal sentido, se puede apreciar cómo el legislador español ha rehuído calificar este tipo de contratos. Sin embargo, en el art. 59.4 TRLGDCU se hace referencia a “(...) los contenidos o servicios digitales objeto de un contrato de compraventa o de servicios”, de lo que podemos inferir que, evidentemente, el suministro de contenidos o servicios digitales, en algunas ocasiones, adoptará la forma de un contrato de compraventa y, en otras, la de un contrato de servicios, pero ello no excluye que el suministro de contenidos o servicios digitales pueda adoptar otras formas como un contrato de alquiler o un contrato de obra (v.g. contrato de creación de una página web conforme a las especificaciones del consumidor), en cuyo caso, consideramos que también deberían aplicarse las normas del TRLGDCU.
- 18 Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (ELI: <http://data.europa.eu/eli/dir/2019/770/oj>).

De esta forma, quedarían sujetos a la DCSD y al TRLGDCU aquellos supuestos en los que el consumidor, por ejemplo, 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 quedarán sujetos los casos en los que el consumidor da su consentimiento para que cualquier material que constituya datos personales, como fotografías o mensajes que cargue, sea tratado por el empresario con fines comerciales.

Es importante detenerse en esta diferenciación que se realiza entre los contratos en los que el consumidor abona un precio y aquellos otros en los que la contraprestación consiste en la facilitación de datos personales por parte del consumidor o usuario, y cuya inclusión se previó con la finalidad de evitar que, dependiendo de la naturaleza de la contraprestación, se generase una discriminación entre los diferentes modelos de negocio, así como rehuir de incentivos injustificados a las empresas para orientarse hacia la oferta de contenidos digitales a cambio de datos¹⁹.

Así, por un lado, nos encontramos con aquellos contratos en los que el empresario que suministra el contenido o servicio digital recibe como contraprestación un precio²⁰; y, por otro lado, aquellos contratos en los cuales el empresario que suministra contenidos y servicios digitales recibe como contraprestación la cesión de uso de los datos personales por parte del consumidor y usuario²¹. Esta ha sido

19 Esta es la razón que señalaba el Cdo. 13 de la Propuesta de Directiva del Parlamento Europeo y del Consejo, sobre determinados aspectos de los contratos de suministro de contenidos digitales [COM (2015) 634 final] (en adelante, PropDCSD).

20 El legislador europeo reconoce en el art. 3.1 DCSD la aplicación de la Directiva “a todo contrato en virtud del cual el empresario suministra o se compromete a suministrar contenidos o servicios digitales al consumidor y este paga o se compromete a pagar un precio”. Sin embargo, no encontramos su homónimo en el TRLGDCU, aunque el reconocimiento del pago de un precio en dinero como contraprestación del contrato de suministro de contenidos y servicios digitales puede deducirse a partir de algunos de sus preceptos, que contienen varias referencias expresas al pago de un precio en este tipo de contratos. Sin ir más lejos, el art. 117.1, párrafo 1º TRLGDCU reconoce como medida correctora, en caso de falta de conformidad del contenido o servicio digital, la reducción del precio, la cual solo puede tener cabida cuando se paga una cantidad de dinero determinada o determinable. En la misma línea, el párrafo 2º del mismo precepto faculta al consumidor a suspender cualquier parte pendiente del precio del contenido o servicio digital hasta que el empresario cumpla con su obligación. Por su parte, el art. 119 bis. 2 TRLGDCU hace referencia a los contenidos o servicios digitales que “se suministren durante un período de tiempo a cambio del pago de un precio (...)”, por lo que es evidente que se reconoce el pago de un precio como contraprestación en este tipo de contratos. No obstante, si bien es cierto que el TRLGDCU no especifica qué debe entenderse por precio, sí lo hace la DCSD, que contiene su definición en el art. 2.7, conforme al cual se entiende por precio “el dinero o una representación digital de valor”. Por todo ello, cabe considerar que la contraprestación consistente en la cesión de uso de datos personales no tendría encaje bajo la definición de precio. Sin embargo, parte de la doctrina más autorizada como DE FRANCESCHI, “Personal Data as Counter...”, cit., p. 63, propone que el concepto de “precio” debería actualizarse teniendo en cuenta las necesidades de la economía digital. En tal sentido, el autor sugiere que debería incluirse en el mismo a los datos personales que se ceden como contraprestación. Aunque, tal y como está configurado el espectro normativo actualmente, no debe confundirse el pago de un precio con la cesión de datos personales, y ello con independencia de que estén sometidos, aunque con matices, a las mismas reglas.

21 Como señala ROSELLÓ RUBERT, F.M.: “La propuesta de Directiva sobre suministro”, cit., p. 275, la falta de contraprestación dineraria no supone en modo alguno que estas relaciones jurídicas no sean vinculantes y exigibles para las partes, sino que, al contrario, estamos pues ante contratos vinculantes.

una de las novedades más relevantes de la DCSD, aunque se trata de una solución que ya se preveía en el art. 5, letra b) de la fracasada Propuesta del CESL²². Sin embargo, hay que tener en cuenta que la DCSD eliminó de su texto normativo cualquier referencia expresa al término “contraprestación” en relación con los datos personales debido a las fuertes críticas que recibió por parte del Supervisor Europeo de Protección de Datos (en adelante, SEPD) en su Dictamen 4/2017²³. Por el contrario, la PropDCSD sí que aludía al suministro a cambio de que el consumidor facilitase “activamente otra contraprestación no dineraria en forma de datos personales u otro tipo de datos”. La razón por la que el SEPD instaba la eliminación del término “contraprestación” era que tal denominación podía afectar a la naturaleza del derecho fundamental de protección que recae sobre los datos facilitados.

Ahora bien, el hecho de que la DCSD en su Cdo. 24 señale que “la protección de datos personales es un derecho fundamental, por lo que los datos personales no pueden considerarse una mercancía”²⁴, no significa que estos no puedan considerarse como contraprestación del suministro de contenidos o servicios digitales, pues, simplemente, el legislador europeo ha utilizado una fórmula más conservadora y reticente (“facilite o se comprometa a facilitar datos personales al empresario”), lo que no priva a los mismos de la posibilidad de que sean considerados como “contraprestación”. Por tanto, los cambios tan significativos que podemos apreciar en el tenor literal del texto en la DCSD respecto a la

Vid., en la misma línea, GARCÍA HERNÁNDEZ, A.: “Datos personales como contraprestación: consecuencias”, *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2021, p. 8, (<http://centrodeestudiosdeconsumo.com/index.php/2-principal/5289-datos-personales-como-contraprestacion-consecuencias>), afirma que la contraprestación de un servicio o de un bien puede consistir en métodos de pago distintos al propio dinero, a pesar de constituir este el elemento paradigmático que representa la contraprestación clásica en el sistema negocial actual, por lo que el pago con datos personales constituye una auténtica contraprestación, dando lugar a verdaderos contratos onerosos y no a título gratuito como cabría pensar; y FERNÁNDEZ PÉREZ, N.: “Contrato sobre contenidos o servicios digitales con consumidores a cambio de datos”, en AA.VV.: *Contratación mercantil: digitalización y protección del cliente-consumidor* (dir. por L.M. MIRANDA SERRANO y J. PAGADOR LÓPEZ), Marcial Pons, Madrid, 2023, p. 58, quien señala que si los datos no fueran una contraprestación, y tampoco se entregara precio, no podríamos hablar de la existencia de una relación contractual regulada por la normativa de consumidores.

- 22 De acuerdo con el art. 5, letra b) de la Propuesta del CESL dicha normativa podía aplicarse a “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”. Como se puede apreciar, no se hacía una referencia expresa a los datos personales, pero cabía la posibilidad, dado que contemplaba no solo contraprestaciones a cambio de precio, sino también aquellas que no consistieran en el pago de un precio en dinero. De hecho, el Cdo. 18 CESL hacía referencia a que los contenidos digitales, a menudo, 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. Y añade que “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”.
- 23 European Data Protection Supervisor, Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, Dictamen núm. 4/2017, 14 de marzo de 2017, pp. 1-26. (Consultar en: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf).
- 24 De la misma manera lo establece el Real Decreto-ley 7/2021 en su Exposición de Motivos.

versión –originaria- de la PropDCSD a raíz de las críticas del SEPD, son cambios fundamentalmente terminológicos y no tanto sustantivos.

Por otro lado, a diferencia de lo establecido por la DCSD en su Cdo. 24, es curioso como en el ámbito del derecho tributario no ocurre lo mismo, ya que la Exposición de Motivos de la Propuesta de Directiva del Consejo relativa al sistema común del impuesto sobre los servicios digitales que grava los ingresos procedentes de la prestación de determinados servicios digitales, de 21 de marzo de 2018²⁵, señala que los usuarios pueden contribuir a generar valor para las empresas digitales. En este sentido, indica que “las empresas digitales pueden obtener datos sobre las actividades de los usuarios en las interfaces digitales que suelen servir para ofrecer a esos usuarios publicidad específicamente destinada a ellos, o que pueden transmitirse a terceros a título oneroso”²⁶. No obstante, si bien es cierto que esta propuesta de la Comisión Europea fue finalmente rechazada al no alcanzarse la unanimidad requerida para su aprobación, el legislador español se anticipó a los debates internacionales –que no aportaron soluciones prácticas al respecto- y adoptó de forma unilateral –como otros tantos países- una solución que permitió a España ejercer de forma inmediata derechos de imposición que legítimamente le corresponden, por ser de donde proceden “los datos y las contribuciones de los usuarios que generan valor a la empresa”. Así, se procedió al regular el Impuesto sobre Determinados Servicios Digitales en la Ley 4/2020, de 15 de octubre, del Impuesto sobre Determinados Servicios Digitales²⁷, el cual tiene por objeto las prestaciones por servicios digitales en relación con los cuales existe una participación de los usuarios que “constituye una contribución al proceso de creación de valor de la empresa que presta los servicios, y a través de los cuales la empresa monetiza esas contribuciones de los usuarios”. En este sentido, el impuesto grava, entre otras, la transmisión, incluidas la venta o cesión, de los datos recopilados acerca de los usuarios que hayan sido generados por actividades desarrolladas por estos últimos en las interfaces digitales, lo que se denomina servicios de transmisión de datos²⁸.

25 Consultar en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52018PC0148>

26 Y, en un sentido similar, también nos parece oportuno traer a colación las palabras de la Comisión Europea en su Documento de Trabajo *Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication Building a European data economy*, Bruselas, 10.I.2017. COM (2017) 9 final, p. 12 (Consultar en: <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>), donde reconoce que existe un mercado de datos entre empresas y, en consecuencia, afirma que las empresas deberían poder obtener datos como cualquier otro recurso físico lo que, al mismo tiempo, les permite monetizar ciertos datos que poseen abriendo fuentes de ingresos adicionales.

27 Consultar en: <https://www.boe.es/eli/es/l/2020/10/15/4>

28 Los servicios de transmisión de datos se definen por el art. 4.8 de la Ley 4/2020 como “los de transmisión con contraprestación, incluidas la venta o cesión, de aquellos recopilados acerca de los usuarios, que hayan sido generados por actividades desarrolladas por estos últimos en las interfaces digitales”. Para un análisis exhaustivo de este impuesto, *vid.*, a este respecto, PÉREZ MERINO, Christian, *El impuesto sobre determinados servicios digitales: la respuesta a la cuarta revolución industrial*, Tirant lo Blanch, Valencia, 2023, pp. 87-207.

Como se puede apreciar, la legislación tributaria –tanto en la referida Propuesta como en la nueva Ley 4/2020– sí reconoce el pago por parte del usuario con sus datos personales, pues lo que pretende gravar es el beneficio que las empresas digitales obtienen de la venta de dichos datos personales cedidos como contraprestación. De esta forma, se pone de manifiesto cómo las expresiones a las que se refiere la DCSD para evitar el reconocimiento expreso de los datos personales como contraprestación son cuestiones meramente terminológicas con poca relevancia en cuanto a su sustantividad, pues la Unión Europea y los Estados miembros son plenamente conscientes de que en el *modus operandi* de los mercados digitales la cesión de los datos personales constituye una pieza angular como contraprestación en cada vez más contratos.

Además, los tribunales también están empezando a reconocer el carácter contractual de estas relaciones entre proveedores y usuarios cuando la contraprestación consiste en la cesión de uso de datos personales.

Así, la sentencia del Tribunal de Grande Instance (TGI) de París, de 9 de abril de 2019²⁹, mostró su rechazo a la alegación de *Facebook* de que sus contratos no estaban sometidos a la Directiva 93/13 sobre cláusulas abusivas³⁰, ya que los mismos debían ser considerados como gratuitos. El argumento del TGI fue que los datos que *Facebook* recaba de sus usuarios son monetizados con terceros por lo que existe una “ventaja” conforme al art. 1.107 del CC francés³¹ y, en consecuencia, el contrato concluido por *Facebook* con sus usuarios debe ser considerado como un contrato oneroso.

En la misma línea, la SAP de Baleares (sec. 3^a), de 26 de marzo de 2020³², afirma que el Acuerdo de Usuario firmado entre *Twitter* y sus usuarios es un “contrato que vincula a ambas (partes) y establece una serie de derechos y obligaciones para cada una de ellas, recogiendo también las consecuencias de esos incumplimientos”. Como es sabido, en el caso de *Twitter*, los usuarios no pagan un precio en dinero, sino que la contraprestación consiste en la cesión de uso de sus datos personales, por lo que, en este supuesto, también se está admitiendo la posibilidad de este tipo de contraprestación, toda vez que se reconoce su carácter contractual.

29 Consultar la decisión completa del TGI en: <https://www.doctrine.fr/d/TGI/Paris/2019/KFV477F659FC5AF0E0B8DD8>

30 Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (Consultar en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-1993-80526>)

31 Art. 1.107 CC francés: “Le contrat est à titre onéreux lorsque chacune des parties reçoit de l'autre un avantage en contrepartie de celui qu'elle procure. Il est à titre gratuit lorsque l'une des parties procure à l'autre un avantage sans attendre ni recevoir de contrepartie”.

32 SAP de Baleares (Sección 3^a), de 26 de marzo de 2020 (ECLI: ES:APIB:2020:513).

Más recientemente, el Juzgado de lo Mercantil de Barcelona³³ en un caso donde un usuario pretendía recuperar su cuenta de *Twitter*, a la que no podía acceder por haber olvidado su contraseña y estar asociada a una dirección de correo electrónico que ya había sido dada de baja, el Juzgado reconoce el “acuerdo o contrato” que vincula al usuario con la plataforma.

También puede resultar interesante una resolución de 29 de noviembre de 2018 de la *Autorità Garante della Concorrenza e del Mercato* italiana, la cual impuso una multa de 10 millones de euros a *Facebook* por haber suministrado a los usuarios información que no era adecuada para generarles suficiente conciencia sobre el uso que iba a realizarse de los datos personales que habían facilitado. En concreto, señaló que, en la primera página de registro, la información señalaba que el servicio era gratuito y no se hacía referencia a fines comerciales para los que iban a ser utilizados, por lo que dicha información carecía de claridad, inmediatez e integridad. En tal sentido, la Autoridad obligó a *Facebook* a modificar la información que aparecía en la página del sitio web, entre la que se encontraba la referencia a la “gratuidad” del servicio.

Por su parte, el legislador español, al transponer la DCSD al TRLGDCU, sí que ha hecho referencia expresa en el art. 119 ter. 2 TRLGDCU a los “supuestos en que el consumidor o usuario haya facilitado datos personales como contraprestación”³⁴. Se puede apreciar como aquí el legislador nacional se ha desmarcado de esas consideraciones de la DCSD³⁵ y reconoce expresamente a los datos personales naturaleza de contraprestación contractual.

Por el contrario, una parte de la doctrina³⁶ se ha planteado la dudosa posibilidad de comercialización de los datos personales, dado que estos podrían entrar en conflicto con lo dispuesto en el art. 1.271 CC el cual señala que “pueden ser objeto

33 SJMerc nº 2 de Barcelona, de 15 de marzo de 2022 (ECLI: ES:JMB:2022:2483).

34 Como acertadamente señala FERNÁNDEZ CHACÓN, I.: “Caracterización y régimen aplicable a los contratos de suministro de contenidos y servicios digitales”, en AA.VV.: *El nuevo derecho digital: I. Los contratos de suministro de contenidos y servicios digitales* (dir. por: F. GÓMEZ POMAR e I. FERNÁNDEZ CHACÓN), Aranzadi, Madrid, 2024, p. 321, nota 287, lo preceptuado en este artículo presenta una evidente incoherencia con las reflexiones contenidas en la Exposición de Motivos del RDL 7/2021 sobre la no equiparación entre los datos personales y otras mercancías y, por tanto, la imposibilidad de que la cesión de uso de los datos personales pueda entenderse como una contraprestación propiamente dicha.

35 Se muestra muy crítico con este cambio CASTILLO PARRILLA, J.A.: “Los datos personales como contraprestación en la reforma del TRLGDCU y las tensiones normativas entre la economía de los datos y la interpretación garantista del RGPD”, *La Ley Mercantil*, núm. 82, 2021, pp. 10 y 17, quien afirma que la expresión introducida por el TRLGDCU no es solamente contraria a una afirmación clara de la Directiva 2019/770, sino que también es contraria a la opinión de la Autoridad de la UE encargada de defender el cumplimiento de la normativa de datos personales. Por ello, el autor insta al legislador a que suprima esta expresión del art. 119 ter. 2 TRLGDCU, respetando así los criterios (terminológicos al menos) de una de las Directivas que se transponen. Esto debe hacerlo tanto si la inclusión de dicha expresión ha sido un descuido fruto de las prisas como si ha sido intencionada, dado que una norma de transposición no es el cauce para defender una postura distinta de la que ya ha cristalizado en la norma objeto de transposición.

36 GARCÍA HERRERA, V.: “El pago con datos personales. Incoherencias legislativas derivadas de la configuración de los datos como posible ‘contraprestación’ en el suministro de contenidos y servicios digitales”, *Actualidad Civil*, núm. 1, 2020, p. 6.

de contrato todas las cosas que no están fuera del comercio de los hombres". En consecuencia, como la protección de los datos personales aparece configurada como un derecho fundamental y, por ende, sustraído de la disponibilidad de los particulares, los datos personales no pueden ser objeto del contrato ya que no se hallan comprendidos en el patrimonio y, por tanto, no pueden ser utilizados como moneda de cambio, al ser considerados como *res extra commercium*.

Sin embargo, desde nuestro punto de vista, consideramos que no debería excluirse la posibilidad de que el consumidor explotase sus datos personales y, por tanto, los utilizase como contraprestación en el tráfico jurídico³⁷. Efectivamente, si bien es cierto que nos encontramos ante un derecho de la personalidad —y, por tanto, indisponible— no se está disponiendo completamente de este derecho, sino solamente de forma parcial, en su dimensión patrimonial³⁸, esto es, autorizando su acceso a su esfera de exclusividad³⁹. De hecho, ese carácter de "indisponibilidad" de la información personal que se postula, desde la teoría clásica sobre los "bienes de la personalidad", esfera a la cual pertenecería dicha información, podría salvarse distinguiendo entre la titularidad de la información personal, de la cual no se desprendería nunca el individuo, y las facultades que la integran, en particular, la facultad de uso para cederla a terceros mediante la celebración de contratos⁴⁰. En nuestro Derecho hay casos similares en los que se admite un acto de disposición parcial de un derecho propio de la personalidad (como el derecho a la intimidad

37 De la misma opinión es MARTÍNEZ CALVO, J.: "Los datos personales como posible contraprestación en los contratos de suministro de contenidos y servicios digitales", *Indret: Revista para el Análisis del Derecho*, núm. 4, 2021, p. 101, así como GARCÍA HERNÁNDEZ, V.: "Los datos como contraprestación o la pérdida encubierta de la privacidad del individuo a cambio de 'servicios gratuitos'", *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2022, pp. 1-2 (Disponible en: http://centrodeestudiosdeconsumo.com/images/Los_datos_como_contraprestacion.pdf).

38 *Vid.*, en el mismo sentido, CÁMARA LAPUENTE, S.: "Extinción de los contratos", cit., p. 179; RICCIUTO, V.: "Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali", *Rivista di diritto civile*, vol. 66, núm. 3, 2020, pp. 642 y ss.; y GARCÍA HERRERA, V.: "El pago con datos personales", cit., p. 7, quien afirma que el hecho de que el derecho a la protección de los datos de carácter personal sea un derecho fundamental, no impide que el mismo sea "disponible" en su dimensión económica. Nada obsta a que, de la misma manera que resulta posible explotar patrimonialmente otros aspectos de la personalidad, como la imagen y la intimidad, "disponiendo" de ellos a cambio de una contraprestación económica, podamos del mismo modo "disponer" de nuestros datos a cambio de un contenido o de un servicio digital.

39 MARTÍNEZ VELENCOSO, L.M. y SANCHO LÓPEZ, M.: "El nuevo concepto de onerosidad", cit., p. 10.

40 Al respecto, como acertadamente señala NAVAS NAVARRO, S.: "El valor de los datos personales", cit., pp. 106-107, otorgando valor a los datos personales y reconociendo derechos a favor de su titular se está también protegiendo su dignidad y su derecho a la privacidad. *Vid.* igualmente, PLANA ARNALDOS, M.C. "Los datos personales como contraprestación", en AA.VV.: *Protección de Datos Personales* (coord. por I. GONZÁLEZ PACANOWSKA), Tirant lo Blanch, Valencia, 2020, p. 574.

o a la propia imagen)⁴¹ a cambio de una contraprestación económica⁴², es decir, que la decisión sobre la explotación económica de la privacidad pertenece al titular de tales derechos. En consecuencia, si se niega la disponibilidad del aspecto patrimonial de este derecho al titular de los datos, ello supondría una falta de coherencia⁴³, pues esta diferencia de trato respecto a los demás derechos de la personalidad -como el derecho a la intimidad o a la propia imagen- carecería de toda lógica y justificación.

De esta forma, defendemos que, aunque la protección de datos personales se erija como derecho fundamental ligado a los derechos de la personalidad, ello no es incompatible con que puedan ser objeto de comercialización, es decir, que en su dimensión monetaria, los titulares sean libres de explotarlos económicamente⁴⁴. Aunque, no obstante, es cierto que lo conveniente en estos casos pasa por limitar

- 41 Vid., por ejemplo, STC (Sala) 117/1994, de 25 de abril de 1994 (núm. 117/1994, 31 de mayo de 1994) (ECLI:ES:TC:1994:117), la cual señala que “los artistas profesionales del espectáculo (o quienes pretenden llegar a serlo) (...) consienten con frecuencia la captación o reproducción de su imagen, incluso con afección a su intimidad, para que pueda ser objeto de explotación comercial”. Vid., en un sentido similar, STS 266/2016, Sala de lo Civil, de 21 de abril de 2016 (ECLI:ES:TS:2016:17790). Por el contrario, en opinión de DE VERDA Y BEAMONTE, J.R.: “El derecho a la propia imagen”, en AA.VV.: *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen* (coord. por J.R. DE VERDA Y BEAMONTE, Aranzadi, Cizur Menor (Navarra), 2007, pp. 174-175, no puede hablarse de un acto de disposición en sentido estricto, ni siquiera parcial de las facultades que integran un derecho de la personalidad; y ello aunque el consentimiento se preste a cambio de una compensación económica. Por ello, el citado autor considera que la explicación más correcta es la que ve en dicho consentimiento un acto de autonomía de la persona, que determina la licitud de una conducta, que, de no mediar la autorización del titular, sería ilegítima. Sin embargo, esta tesis defendida por el profesor DE VERDA Y BEAMONTE, salvando algunas consideraciones, creemos que tampoco se aleja mucho de nuestra postura (que defendemos más adelante), en virtud de la cual cabe separar el consentimiento contractual y el consentimiento conforme al RGPD, de manera que la ilicitud de este último consentimiento no debe afectar al consentimiento contractual y, en consecuencia, no afectar a la validez del contrato celebrado. Esta misma razón es la que lleva a considerar que una retirada del consentimiento al tratamiento de los datos personales tampoco tiene por qué afectar necesariamente a la validez del contrato.
- 42 Así lo pone de manifiesto también TRIPODI, E.M.: “Consumi digitali e dati personali”, cit., p. 276, quien señala que sobre la “monetización” de los datos personales (imagen, voz, rostro, etc.) de los derechos de la personalidad, muchas personas famosas (actores, futbolistas, personajes del mundo del espectáculo) han construido desde hace mucho tiempo relaciones de patrocinio, branding, co-marketing y otras figuras similares, sin que esto haya generado importantes preocupaciones. También hace alusión a estos precedentes CONESA CABALLERO, O.: “El encaje contractual de la cesión de datos de carácter personal: A propósito de la directiva 2019/770 sobre contratos de suministro de contenidos y servicios digitales”, *InDret: Revista para el Análisis del Derecho*, núm. 2, 2024, p. 142.
- 43 Vid., en la misma línea, PACHECO JIMÉNEZ, M.N. y LEAL CORONADO, M.: “Nueva moneda de cambio: Nuestros datos personales como pago de contenidos digitales”, *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2017, p. 4.
- 44 Vid., en el mismo sentido, METZGER, A., et al., “Data-Related Aspects of the Digital Content Directive”, *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 9, núm. 1, 2018, p. 94; o ARTIGOT GOLOBARDES, M.: “La contratación digital con consumidores en dos actos: las políticas de privacidad en la antesala de la contratación digital”, en AA.VV.: *Estudios de Derecho Contractual Europeo: nuevos problemas, nuevas reglas* (dir. por F.GÓMEZ POMAR E I. FERNÁNDEZ CHACÓN), Aranzadi-Thomson Reuters, Cizur Menor (Navarra), 2022, p. 468, quien señala que un modelo basado en la autonomía privada supone que los datos personales pueden ser objeto de derecho reales, concretamente del derecho de propiedad, como cualquier otro bien mueble o inmueble, sobre el cual el individuo puede ejercer potestades propias del derecho de propiedad y decidir lo que considere. Y, en este mismo sentido, también se postula SOLOVE, D.J.: “Privacy Self-Management and the Consent Dilemma”, *126 Harvard Law Review* 1880, núm. 141, 2013, pp. 1180-1903. Por el contrario, COFONE, I.: “Beyond Data Ownership”, *Cardozo Law Review*, vol. 43, núm. 2, 2021, pp. 524-29, se muestra crítico con el enfoque de propiedad de la información personal y, en consecuencia, afirma que la idea de propiedad sobre los datos personales aleja al consumidor de una mayor protección.

la autonomía privada con la finalidad de proteger al titular del derecho⁴⁵. Así, el régimen ordinario del Derecho contractual debería de adaptarse en aras a la protección de estos derechos de la personalidad susceptibles de comercialización⁴⁶ y, para que ello sea posible, se debería tratar de buscar un compromiso entre el Derecho patrimonial y el deber público de proteger la dignidad humana y los derechos fundamentales, del cual se derive la adecuada solución a los problemas suscitados, tanto en su vertiente económica, como en la más genuinamente personal⁴⁷.

Por su parte, cabe añadir que no solo no existe ninguna norma que excluya la posibilidad de que los datos personales puedan constituir una contraprestación en el comercio⁴⁸, sino que la DCSD no prevé en su articulado ninguna exclusión de los mismos del comercio⁴⁹. Es más, llega a admitirlos como instrumento de pago, por lo que pueden ser objeto del contrato al estar dentro del comercio. De hecho, se puede decir que la propia DCSD sí reconoce la vertiente patrimonial de los datos personales, ya que establece medidas correctoras para aquellos casos en los que el consumidor da su consentimiento para el tratamiento y los cede a cambio de contenidos y servicios digitales⁵⁰; y, siguiendo esta idea, como ya hemos

- 45 Una opción razonable sería contar con alguna forma de control *a posteriori* por parte de los poderes públicos que, junto con el consentimiento previo del interesado, pudiese generar un sistema que protegiera adecuadamente los intereses de ambas partes. Precisamente, este control llevado a cabo posteriormente por los poderes públicos encontraría sus motivos en que el interesado cuando da su consentimiento para el tratamiento de sus datos personales no puede ser consciente del alcance del mismo, pues esos mismos datos del usuario serán agregados a otros datos de terceros que generarán una información futura de gran valor y que, el individuo, en el momento de evaluar y aceptar la política de privacidad le es imposible conocer.
- 46 MARTÍNEZ VELENCOSO, L.M. y SANCHO LÓPEZ, M.: “El nuevo concepto de onerosidad”, cit., p. 10.
- 47 GARCÍA RUBIO, M.P.: “La huella y el legado de Federico de Castro en la moderna protección civil de los derechos de la personalidad”, en AA.VV.: *Glosas sobre Federico de Castro* (dir. por L.M. DIEZ PICAZO), Aranzadi, Cizur Menor (Navarra), 2015, p. 249.
- 48 *Vid.*, en este sentido, GARCÍA VICENTE, J.R.: “Arts. 1.271-1.272 CC”, en AA.VV.: *Comentarios al Código Civil* (Tomo VII) (dir. por R. BERCOVITZ RODRIGUEZ-CANO), Tirant lo Blanch, Valencia, 2013, p. 9139, quien afirma que las cosas o servicios como objeto del contrato serán lícitas si no están “excluidas por las leyes del tráfico jurídico”.
- 49 Y, en el mismo sentido, podemos hacer referencia al RGPD del cual no se deduce ninguna norma prohibitiva que excluya los datos personales del comercio de los hombres. De hecho, el Cdo. 4 RGPD señala que “El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad”. En tal sentido, como acertadamente apunta DOMÍNGUEZ YAMASAKI, M. I.: “El tratamiento de datos personales”, cit., pp. 101-102, este derecho debe ponerse en relación con el derecho a la libertad de empresa, por lo que no parece que pueda rechazarse la consideración de los datos personales como mercancía, sino que al no haber una norma expresa que excluya la posibilidad de tratamiento de los datos personales con fines comerciales, la conclusión debe ser su admisión. Y que, entonces, lo fundamental es que el tratamiento de datos personales se lleve a cabo conforme a la ley. Es decir, que sea un tratamiento lícito. De igual manera, JANEČEK, V. y MALGIERI, G.: “Data Extra Commercium”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSE, R. SCHULZE y D. STAUDEMANYER), Nomos/Hart, Baden-Baden (Munich), 2020, p. 115, manifiestan que los datos personales no se rigen por ninguna regla de inalienabilidad y, por lo tanto, no son *res extra commercium*. Ahora bien, dado que al flujo de datos personales se le aplican algunas condiciones estrictas, los autores afirman que los datos personales están sometidos a una regla de enajenabilidad dinámicamente limitada.
- 50 ROSELLÓ RUBERT, F.M.: “Las cargas del usuario de servicios de música en continuo (streaming) algunas consideraciones desde la perspectiva de la nueva normativa europea”, en AA.VV.: *Plataformas digitales: aspectos jurídicos* (dir. por A. MARTÍNEZ NADAL), Aranzadi, 2021, pp. 251-252. Aunque cabe matizar, tal y como pone de relieve METZGER, A.: “Un modelo de mercado para los datos personales: estado de la

dicho, el legislador español sí que ha reconocido expresamente su naturaleza de contraprestación contractual, tal y como se desprende del tenor literal del art. 119 ter. 2 TRLGDCU.

Por último, consideramos que si excluyéramos a los contratos en los que se ceden datos personales como contraprestación del ámbito de aplicación de la DCSD y del TRLGDCU, ello conduciría a una diferencia de trato entre aquellos consumidores que pagan un precio en dinero y aquellos que ceden sus datos como contraprestación⁵¹, pues estos últimos resultarían desprotegidos ya que no les serían aplicables los derechos reconocidos en la propia DCSD o el TRLGDCU. Esta posible discriminación, lógicamente, debe evitarse puesto que aquellos que facilitan sus datos personales como contraprestación no están adquiriendo unos contenidos o servicios digitales de forma gratuita y, por tanto, merecen un nivel de protección en cuanto a derechos y garantías equivalente a aquellos consumidores que pagan un precio en dinero.

En este sentido, tampoco existen dudas en que la DCSD y el TRLGDCU se aplicarán a los contratos en que la contraprestación es mixta, es decir, aquellos casos en que el consumidor pague un precio en dinero y facilite datos personales a cambio del suministro de contenidos o servicios digitales⁵², pues la onerosidad del contrato se predica en toda su extensión. De hecho, así lo confirma también el Cdo. 67 DCSD, en el cual se establece que “En los casos en que el consumidor pague un precio y facilite datos personales, el consumidor debe tener derecho a todas las medidas correctoras disponibles en caso de falta de conformidad”. Ahora bien, además de la posible aplicación de las medidas correctoras, el empresario deberá cumplir, respecto de los datos personales, las obligaciones derivadas del RGPD.

En definitiva, dada la indudable naturaleza de los datos personales como contraprestación contractual y el creciente aumento de los modelos de negocio en que son utilizados de esta manera, consideramos conveniente realizar seguidamente un análisis detallado de algunos aspectos relacionados con ellos, que se abordan en los apartados siguientes.

cuestión a partir de la nueva Directiva sobre contenidos y servicios digitales”, en AA.VV.: *El derecho privado en el nuevo paradigma digital* (dir. por E. ARROYO AMAYUELAS y S. CÁMARA LAPUENTE), Pons, Madrid, 2020, p. 139, que la DCSD no tiene como fin establecer un mercado de datos personales, sino que esta se limita a regular un mercado ya existente en la práctica, reconociendo algunos derechos a favor de los consumidores.

51 *Vid.*, en la misma línea, MAK, V.: “The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content – In-depth análisis”, *Publications Office*, 2016, pp. 10-11; LOHSSE, S., et.al., “Data as Counter-Performance – Contract Law 2.0? An Introduction”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSSE, R. SCHULZE y D. STAUDEMANYER), Nomos/Hart, Baden-Baden (Munich), 2020, p. 16; y HACKER “Regulating the Economic Impact...”, cit., p. 61; y FERNÁNDEZ PÉREZ, N.: “Contrato sobre contenidos”, cit., p. 59.

52 Sería el caso, por ejemplo, de los modelos de negocio denominados “Freemium” en los que inicialmente el acceso al contenido o servicio digital se hace a cambio de datos, pero, posteriormente, se debe pagar una cantidad de dinero para tener algunas funcionalidades extra.

III. MARCO JURÍDICO DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ÁMBITO DE LOS CONTENIDOS Y SERVICIOS DIGITALES.

I. Sobre el alcance del derecho a la protección de los datos personales.

El derecho a la protección de datos de carácter personal es un derecho fundamental consagrado por la Constitución española en su artículo 18.4 en el que se indica que “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”⁵³. Si bien es cierto que la mención a la “protección de datos personales” no aparece en el texto, tal ausencia no ha sido un obstáculo para que el Tribunal Constitucional haya ido construyendo un derecho con sustantividad propia⁵⁴. Así, sobre la base del referido artículo se ha ido configurando este derecho a la protección de los datos personales⁵⁵ que refleja la idea de que la persona debe ser consciente y capaz de controlar el destino de sus datos personales, es decir, quién los posee y con qué finalidad⁵⁶.

Este derecho a la protección de los datos personales se ha definido por el Tribunal Constitucional⁵⁷ como “un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”. Y añade, que este derecho fundamental a la protección de datos “no se reduce sólo a los datos

53 Para un mejor análisis sobre el proceso por el cual la protección de datos adquiere el rango de derecho fundamental, *vid.*, AMÉRIGO ALONSO, J.: “Objeto y ámbito de aplicación”, en AA.VV.: *Tratado de protección de datos* (dir. por A. RALLO LOMBARTE), *Tratado de protección de datos*, Tirant lo Blanch, Valencia, 2019, pp. 83-93.

54 *Vid.*, en este sentido, las conocidas SSTC (Sala) 254/1993, de 20 de julio de 1993 (núm. 254/1993, 18 de agosto de 1993) (ECLI:ES:TC:1993:254); (Sala) 11/1998, de 13 de enero de 1998 (núm. 11/1998, 12 de febrero de 1998) (ECLI:ES:TC:1998:11); y (Pleno) 292/2000, de 30 de noviembre de 2000 (núm. 292/2000, 4 de enero de 2001) (ECLI:ES:TC:2000:292), entre otras.

55 Otros autores como, por ejemplo, CONDE ORTIZ, C.: La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad, Dykinson, 2005, p. 27 ss.; o GUERRERO PICO, M.C.: El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal, Thomson Reuters - Civitas, Madrid, 2006, p. 27 ss, hacen referencia a este derecho como el derecho a la autodeterminación informativa. O, por ejemplo, SALGADO SEGUIN, V.: “Intimidad, privacidad y honor en internet”, Telos: cuadernos de comunicación e innovación, núm. 85, 2010, p. 72, se refiere al mismo como derecho a la privacidad. Sea como fuere su denominación, lo importante es que se engloba bajo el art. 18 CE y ello implica que su desarrollo normativo ha de producirse necesariamente por Ley Orgánica y los actos por los cuales se vulnera o se produce una intromisión ilegítima a este derecho deberán resolverse ante los Tribunales mediante un procedimiento especial y sumario. Además, en última instancia, cabe la posibilidad de recurso de amparo ante el Tribunal Constitucional y recurso ante el Tribunal Europeo de Derechos Humanos.

56 Estos motivos son lo que, a juicio de PLAZA PENADÉS, J.: “Aspectos básicos de la protección de datos de carácter personal”, en AA.VV.: *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen* (coord. por J.R. DE VERDA y BEAMONTE), Aranzadi, Cizur Menor (Navarra), 2007, p. 120, justifican la necesidad de recabar un consentimiento previo para el tratamiento y la cesión de datos, de suministrar un adecuado nivel de información sobre los fines perseguidos con el tratamiento o la cesión, de custodiar los datos personales ajenos con un determinado grado de seguridad y de reconocer a las personas cuyos datos han sido tratados los derechos de oposición, acceso, rectificación y cancelación sobre sus datos.

57 STC (Pleno) 292/2000, de 30 de noviembre de 2000 (núm. 292/2000, 4 de enero de 2001) (ECLI:ES:TC:2000:292).

íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal”⁵⁸. De ahí que este derecho también alcanza a aquellos datos personales que sean públicos, ya que por el mero hecho de que sean accesibles a cualquiera, no significa que escapen del poder de disposición del interesado; y, cabe añadir que el que los datos sean de carácter personal, no significa que únicamente estén protegidos aquellos datos relativos a la vida privada o íntima, sino que también quedarán amparados todos aquellos datos que “identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo”.

Por tanto, los datos que son objeto de protección son aquellos que pueden tener incidencia en el ejercicio de los derechos de la persona, esto es, el derecho al honor, a la intimidad, a la vida privada personal y familiar o cualquier otro derecho reconocido constitucionalmente. Sin embargo, no tienen por qué ser solo aquellos reconocidos por la Constitución, sino que el objeto es mucho más amplio llegando incluso –como nos hemos referido– a aquellos datos públicos de la persona que, en su legítimo derecho a disponer de ellos, puede decidir que no trasciendan a terceros. Estos podrían ser datos de carácter alfabético, como el nombre y apellidos, dirección de correo electrónico⁵⁹, número de móvil o el domicilio personal, pero también aquellos de carácter gráfico o sonoro como, por ejemplo, la fotografía de una persona colgada en una web o una red social, así como la grabación de voz de una persona⁶⁰. Del mismo modo, la información que, sobre nuestras aficiones, gustos, opiniones políticas, creencias, etc., podamos

58 De esta forma, como acertadamente afirma PLAZA PENADÉS, J.: “Aspectos básicos de la protección”, cit., p. 120, la protección legal ya no se proyecta sólo sobre los riesgos o peligros de “la informática”, tal y como prevé la CE, sino también sobre el ámbito del tratamiento de datos en sí mismo, entendido como la posibilidad que tiene un tercero de almacenar distintos datos que cruzados y unidos puede revelar un determinado perfil ideológico o conductual que la persona desearía mantener en secreto y dentro de su ámbito de control.

59 Sobre la consideración del correo electrónico como dato personal se pronunció la AEPD en su Informe Jurídico 0437/2010 en el que señala que en “aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, (...) no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso dicha dirección ha de ser considerada como dato de carácter personal”. Por ejemplo, aquellos supuestos en los que en la dirección de correo electrónico se hace constar el nombre o los apellidos del titular. Pero, también aquellos supuestos en que “la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (...) un primer examen de este dato podría hacernos concluir que no nos encontramos ante un dato de carácter personal”. No obstante, añade que “Sin embargo, incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación”. Por ejemplo, cuando el código de la cuenta de correo va referido a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno, por lo que, en conclusión, el correo electrónico es un dato personal a todos los efectos.

60 Así lo ha reconocido la STS 815/2020 (Sala de lo Civil), de 18 de junio de 2020 (ECLI: ES:TS:2020:1771).

divulgar en la red, bien directamente (v.gr., escribiendo una entrada en un blog) o indirectamente (v.gr., consultando páginas webs relacionadas con nuestros hobbies, que disponen de *cookies*), ha de ser considerada como dato de carácter personal siempre que, de manera aislada o junto con otros datos (v.gr. dirección IP), permita que seamos identificados⁶¹.

En cualquier caso, para que los datos personales sean objeto de protección por el RGPD han de ser datos referidos a “toda información sobre una persona física identificada o identificable”⁶². Por persona física identificada o identificable debemos entender “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”⁶³. En consecuencia, los principios previstos en la normativa de protección de datos personales no serán de aplicación cuando nos encontremos ante información anónima o anonimizada. Ello ocurrirá cuando la persona física (el interesado) no sea una persona identificable o haya dejado de serlo⁶⁴.

De hecho, en relación con los nuevos datos elaborados a partir de datos de carácter personal a través de los algoritmos que se utilizan en las técnicas de Big data, es importante distinguir dos situaciones: 1) Si los nuevos datos resultantes obtenidos a partir de datos personales se refieren a un individuo identificado o identificable, estarán protegidos por el derecho fundamental a la protección de

61 SANTOS MORÓN, M.J.: “Consumidor y nuevas tecnologías”, cit., p. 305.

62 Es la definición de datos personales que ofrece el art. 4.1 RGPD al cual se remite el art. 2.8 DCSD. En el mismo sentido, *vid.*, art. 59 bis, letra h) TRLGDCU. Como puede apreciarse, la protección que otorga el RGPD se aplica únicamente respecto a las personas físicas, quedando excluidas de esta forma las personas jurídicas. En tal sentido lo establece el Cdo. 14 RGPD, el cual señala que “La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas (...)”. Sin embargo, a juicio de PLAZA PENADÉS, “Aspectos básicos de la protección...”, cit., p. 121, la exclusión de las personas jurídicas del ámbito de protección de datos de carácter personal parte de una premisa equivocada en la que se cree que todos los datos de las empresas y demás personas jurídicas son públicos. Además, el autor añade que se desconoce que el daño derivado del tratamiento erróneo de los datos es el mismo en las personas físicas que en las jurídicas y que, en consecuencia, deberían de disponer de los mismos derechos de acceso, rectificación y cancelación de los datos.

63 Sobre el concepto de “identificabilidad” y los criterios aplicables para la identificación, *vid.*, IRTI, C.: “Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data”, en AA.VV.: *Privacy and Data Protection in Software Services* (coord. por R. SENIGAGLIA, C. IRTI y A. BERNES), Signapur, 2022, pp. 50-51.

64 Así lo prevé también el Cdo. 26 RGPD el cual afirma que “los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo”. IRTI, C.: “Personal Data”, cit., p. 52, afirma que la anonimización es una forma de procesamiento de datos destinada a la desidentificación. En tal sentido, señala la autora que por desidentificación debemos entender el proceso por el cual se elimina u oculta cualquier información personal identificable de los registros individuales de manera que se minimice el riesgo de revelación involuntaria de la identidad de las personas y de la información sobre ellas.

datos de carácter personal y, en consecuencia, si el titular de los datos ejercita válidamente su derecho al olvido, éstos deberán ser suprimidos. 2) En cambio, si los nuevos datos han sido elaborados a partir de datos personales de individuos, pero se refieren al público en general y no se asocian a ninguna persona en particular, no tendrán la consideración de datos de carácter personal y, por tanto, no tendrán que ser cancelados⁶⁵.

2. Normativa aplicable a la protección de los datos personales.

En lo que respecta a la protección de datos personales en el contrato de suministro de contenidos y servicios digitales, habrá que tener en cuenta, principalmente, dos normativas. Así, el art. 114.1, párrafo 2º TRLGDCU señala que “El Reglamento (UE) 2016/679, General de Protección de Datos, así como la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y su normativa de desarrollo, se aplicarán a cualesquiera datos personales tratados en las relaciones contempladas en los apartados anteriores, prevaleciendo sus disposiciones en caso de conflicto con lo regulado en este Título”. Por tanto, a los datos personales tratados en relación con un contrato de suministro de contenidos y servicios digitales les resultará de aplicación, de acuerdo con el citado precepto, el RGPD y la Ley 9/2014, General de Telecomunicaciones y su normativa de desarrollo⁶⁶; y, en caso de conflicto entre la normativa de consumo y la normativas de protección de datos personales, prevalecerán estas últimas. No obstante, conviene advertir que la Ley 9/2014 ha sido derogada y, en consecuencia, sustituida por la Ley 11/2022, de 28 de junio, General de Telecomunicaciones⁶⁷, por lo que la ley aplicable a los datos personales será esta última, en lugar de la Ley 9/2014. Por su parte, la

65 *Vid.*, en este sentido, TORRE DE SILVA Y LÓPEZ DE LETONA, J.: “El derecho civil de los datos”, *Anuario de derecho civil*, vol. 72, núm. 3, 2019, pp. 850-851, quien pone un ejemplo bastante ilustrativo: “Cuando un programa de inteligencia artificial ha aprendido sobre el comportamiento de los usuarios de una plataforma por su interacción con los mismos, aunque dichos usuarios se den de baja de la plataforma y ejerciten su derecho al olvido, no resultará en principio obligado que el programa de inteligencia artificial “desaprenda” lo que ha aprendido en relación con la naturaleza humana o con el comportamiento de los usuarios de una plataforma, genéricamente considerados y no identificables. Se tratará de datos de carácter no personal, normalmente no protegidos”.

66 Existen también otras normativas. En concreto: el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1/247/2002/CE (ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>); y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos (ELI: <http://data.europa.eu/eli/dir/2016/680/2016-05-04>). Aunque, como señala MARTÍNEZ CALVO, J.: “Los datos personales”, cit., p. 93, nota 5, se trata de normativas con poca o nula incidencia en esta materia.

67 Consultar en <https://www.boe.es/eli/es/l/2022/06/28/11/con>. En concreto, la Ley 9/2014 ha sido derogada por la letra a) de la disposición derogatoria única de la Ley 11/2022, en la cual se establece que “la Ley 9/2014, de 9 mayo, General de Telecomunicaciones, a excepción de su disposición adicional decimosexta y las disposiciones transitorias séptima, novena y duodécima. No obstante, la derogación de las disposiciones finales primera, segunda, tercera, cuarta, quinta y séptima de la Ley 9/2014, de 9 de mayo, no afectará a los contenidos de las normas legales modificadas por las mismas, que se mantienen en sus términos actualmente vigentes”.

DCSD también señala en su art. 3.8 que “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 I”, es decir, los contratos de suministro de contenidos y servicios digitales. “En particular, la presente Directiva se entenderá sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE (...)”⁶⁸. El contenido de la Directiva 2002/58/CE⁶⁹, más comúnmente conocida como Directiva sobre la privacidad y las comunicaciones electrónicas, se recoge en la nueva Ley 11/2022, General de Telecomunicaciones.

El RGPD es la normativa que proporciona un marco jurídico a la protección de datos personales en toda la Unión Europea, el cual es directamente aplicable y con el que se pretendió poner fin a las distintas divergencias que se producían en la ejecución y aplicación del régimen de protección de datos en los distintos Estados Miembros. Así, el RGPD garantiza un nivel de protección homogéneo para todas las personas físicas de la Unión Europea, protegiendo de una manera más efectiva los datos y el destino de los mismos, toda vez que incorpora nuevos derechos y modifica algunos aspectos relevantes, entre los que destaca, especialmente, el referido al consentimiento del interesado. De esta manera, el consentimiento para el tratamiento de datos personales será lícito cuando se cumplan una serie de requisitos⁷⁰ y el mismo se haya recabado, como se analizará posteriormente, mediante una declaración o una clara acción afirmativa por parte del consumidor o usuario.

Por su parte, a nivel interno, también cabe mencionar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD)⁷¹ la cual ha acogido de forma prácticamente idéntica el régimen del consentimiento previsto en el RGPD. De la misma forma, el art. 119 ter. 5, letra b) TRLGDCU señala que en caso de resolución del contrato, “En lo que respecta a los datos personales del consumidor o usuario, el

68 Cabe destacar la clara concordancia que existe entre la DCSD y el RGPD. Así, por un lado, las disposiciones de la DCSD se aplicarán a cualquier empresa que ejerza su actividad dentro del mercado interior europeo, con independencia de que la misma esté establecida o no en un Estado miembro. Por su parte, las normas de protección de datos previstas en el RGPD (art. 3) se aplicarán a todos los interesados que residan en la Unión Europea, esto es, se aplicarán a todo tratamiento de datos personales que se lleve a cabo en el contexto de actividades de un establecimiento del responsable o del encargado en la Unión Europea, con independencia de que el tratamiento tenga lugar o no dentro de la Unión Europea. E igualmente, serán de aplicación las disposiciones del RGPD a los interesados residentes en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

69 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 (ELI: <http://data.europa.eu/eli/dir/2002/58/2009-12-19>).

70 En particular, habrá que atenerse a los caracteres establecidos en el art. 4.11 del RGPD, es decir, el consentimiento debe ser específico, libre, informado e inequívoco.

71 Consultar en: <https://www.boe.es/eli/es/lo/2018/12/05/3/con>

empresario cumplirá las obligaciones aplicables con arreglo al Reglamento (UE) 2016/679 general de protección de datos, así como a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales⁷².

Finalmente, consideramos importante traer aquí a colación la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores (en adelante, DAR)⁷³, y por la que se deroga la Directiva 2009/22/CE. La DAR impone a los Estados miembros un mandato dirigido a establecer un mecanismo para la defensa -por parte de las entidades habilitadas al efecto- de acciones de representación que se ejerciten frente a actos de los empresarios que infrinjan las disposiciones del Derecho de la Unión Europea que se recogen en el anexo I de la misma, entre las cuales se encuentra la DCSD y el RGPD. Por tanto, en virtud de la DAR, en el marco de un contrato de suministro de contenidos y servicios digitales, cuando exista una falta de conformidad, no solo podrá interponerse una acción colectiva resarcitoria, sino que la entidad habilitada al efecto también podrá interponer una reclamación de indemnización basada en el art. 82 RGPD si se ha constatado la ilicitud del tratamiento de datos personales por parte del empresario o responsable, y todo ello en el marco de la misma acción de defensa colectiva⁷⁴. Ahora bien, cabe advertir que se trata de una Directiva que aún no ha sido transpuesta al ordenamiento jurídico español, para lo cual se requerirá una revisión en profundidad de la tutela colectiva prevista en la Ley de Enjuiciamiento Civil⁷⁵.

IV. EL CONSENTIMIENTO COMO BASE LEGÍTIMA PARA EL TRATAMIENTO DE DATOS PERSONALES.

Para que el tratamiento de los datos personales de un consumidor o usuario -que los cede como contraprestación de un contenido o servicio digital- por parte

72 *Vid.*, en un sentido similar, el art. 107.4 TRLGDCU para el caso de desistimiento.

73 ELI: <http://data.europa.eu/eli/dir/2020/1828/oj>.

74 Para una explicación más exhaustiva de este tipo de acciones de representación colectiva y la interacción entre las distintas normativas europeas *vid.*, PAREDES PÉREZ, J.I.: "Acciones de representación resarcitorias y protección de los consumidores como titulares de datos en los contratos de suministro de contenidos y servicios digitales: un estudio en clave de foros de competencia judicial internacional", en AA.VV.: *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (dir. por. J.J. CASTELLÓ PASTOR), Aranzadi - Thomson Reuters, Cizur Menor (Navarra), 2021, pp. 469-501.

75 Sobre un análisis de los aspectos básicos de la Directiva, *vid.*, en este sentido, MORENO GARCÍA, L.: "La tutela colectiva de los consumidores en la Unión Europea: a propósito de la Directiva 2020/1828, de 25 de noviembre de 2020", *Revista de Derecho Mercantil*, núm. 327, 2023, RR-6.I ss. (consulta online); y LÓPEZ JIMÉNEZ, J.M.: "La protección de los consumidores y las acciones de representación: una primera aproximación a la Directiva (UE) 2020/1828", *Diario la Ley*, núm. 9834, 2021 (consulta online). En cambio, para un análisis de los aspectos procesales básicos que deberán ser objeto de reforma, *vid.*, en este sentido, CHOCRÓN GIRALDEZ, A.M.: "El marco jurídico de la Directiva 2020/1828 en relación con la tutela judicial de los intereses colectivos de los consumidores", *Cuadernos de Derecho Transnacional*, vol. 14, núm. 2, 2022, pp. 275-293; y DE PAZ, S. y DE ARCOS TEJERIZO, M.: "La reforma del sistema de acciones de representación a la luz de la Directiva (UE) 2020/1828", *Revista Jurídica Pérez-Llorca*, núm. 7, 2022, pp. 27-39.

de un tercero resulte lícito, es necesario que concurren las circunstancias previstas en la normativa de protección de datos personales. Como bien señala el Cdo. 24 DCSD “El Derecho de la Unión relativo a la protección de los datos personales establece una lista exhaustiva de motivos legales para el tratamiento lícito de los datos personales”. Por tanto, no es la DCSD la que debe regular las condiciones para que el tratamiento de los datos personales se considere lícito, sino que será el RGPD. En este sentido, como indica el Cdo. 38 DCSD “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”.

En el tipo de contratos que nos ocupa, la licitud del tratamiento se basará, principalmente, en el consentimiento prestado por el consumidor o usuario. Por ello, cuando el tratamiento de datos personales esté basado en el consentimiento, en particular, conforme al art. 6.1, letra a) RGPD, serán de aplicación las disposiciones específicas de dicho Reglamento, incluidas aquellas relativas a las condiciones para determinar si el consentimiento se presta libremente (Cdo. 38 DCSD).

La Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8 señala que el tratamiento de los datos de carácter personal se hará “sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley”. Así, una de las novedades que introdujo el RGPD fue la necesidad que debía mediar el consentimiento del interesado para el tratamiento de datos personales⁷⁶. En este sentido, para que el tratamiento de los datos personales se considere válido, se deberá recabar el consentimiento del interesado con anterioridad al propio tratamiento, ya que se requiere de la aprobación del titular de los datos para que estos puedan ser tratados de una forma válida⁷⁷. Este consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (Cdo. 32 RGPD).

Sin embargo, hay que tener en cuenta que el interesado tendrá derecho a retirar su consentimiento en cualquier momento, sin perjuicio de la licitud del tratamiento de los datos con anterioridad a su retirada (art. 7.3 RGPD). En

76 Por tratamiento de datos personales debemos entender, según el art. 4.2 RGPD, “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.

77 Vid., al respecto, Cdo. 40 RGPD y art. 7.1 RGPD.

consecuencia, si el interesado no goza de una verdadera o libre elección para retirar su consentimiento sin sufrir perjuicio alguno, el consentimiento no puede considerarse libremente prestado. Es por ello que el derecho del consumidor a resolver el contrato conforme al TRLGDCU se entenderá sin perjuicio del derecho a retirar el consentimiento otorgado al tratamiento de datos personales⁷⁸.

Los caracteres definitorios del consentimiento del interesado -libre, específico, informado e inequívoco- establecidos por el RGPD son, idénticamente, seguidos por la LOPDGDD, ya que en su art. 6 hace una remisión al art. 4.II RGPD para definir qué se entiende por consentimiento del interesado. De ahí que la interpretación que hace el TJUE de estos caracteres y la delimitación de las condiciones para que el consentimiento del interesado se considere válido pueda ser perfectamente trasladable a la norma que resulta también de aplicación a nivel nacional como es la LOPDGDD, aparte del RGPD que, como se ha indicado, es directamente aplicable en todos los Estados miembros de la Unión Europea.

Por todo ello resulta de gran interés la doctrina sentada por el TJUE⁷⁹, en el sentido de que viene a interpretar qué debe entenderse por “libre”, “específico”, “informado” e “inequívoco”, caracteres estos que deben presidir cualquier prestación del consentimiento al tratamiento de datos personales por parte del interesado al responsable del tratamiento; y, especialmente, cuando este consentimiento se preste a través de cláusulas insertadas por el responsable del tratamiento de forma predeterminada, como es el caso del tipo de contratos que nos ocupa. Estos requisitos se analizan a continuación.

V. LOS REQUISITOS PARA OBTENER UN CONSENTIMIENTO VÁLIDO.

Tanto el RGPD como la LOPDGDD –por remisión de su art. 6.I al art. 4.II del RGPD- exigen una serie de requisitos para que el consentimiento pueda entenderse válidamente prestado. Se trata del carácter libre, específico, informado e inequívoco que debe tener dicho consentimiento, expresado a través de una declaración o una “clara acción afirmativa”, es decir, se requiere un consentimiento activo. Además, se excluye como consentimiento el prestado a través de las casillas ya marcadas (Cdo. 32 RGPD), porque, como ya ha señalado el TJUE en las referidas sentencias (SSTJUE de 1 de octubre de 2019 y de 11 de noviembre de 2020), es imposible determinar de manera objetiva si el usuario ha prestado efectivamente su consentimiento al tratamiento de sus datos personales al no quitar la marca de una casilla marcada por defecto.

⁷⁸ Vid., en este sentido, el art. 119 ter. 7 TRLGDCU puesto en relación con el Cdo. 39 DCSD.

⁷⁹ Especialmente en las SSTJUE de 1 de octubre de 2019, Asunto C-673/17, *caso Planet 49* (ECLI:EU:C:2019:801), y 11 de noviembre de 2020, Asunto C-611/19, *caso Orange România* (ECLI:EU:C:2020:901).

I. Consentimiento libre.

El art. 4.11 RGPD establece que el consentimiento significa “una manifestación de voluntad libre”. Al respecto, el TJUE⁸⁰ ha afirmado que el carácter libre supone que las estipulaciones contractuales no deben inducir al interesado a error en lo que respecta a la posibilidad de celebrar el contrato pese a su negativa a dar el consentimiento para el tratamiento de sus datos⁸¹. De esta forma, se garantiza una verdadera libertad de elección. A falta de tal información, no puede considerarse que el consentimiento de dicha persona al tratamiento de sus datos personales haya sido dado libremente. En consecuencia, el consentimiento no deberá considerarse libremente prestado cuando el interesado no goza de una verdadera libertad de elección o no puede denegar o retirar su consentimiento sin sufrir ningún perjuicio; y, en el mismo sentido, si bien el RGPD no determina de forma positiva qué es el consentimiento libre, lo hace de forma negativa⁸², concretando que el consentimiento no será libre cuando exista un desequilibrio claro entre el interesado y el responsable del tratamiento, presumiéndose que el mismo no se ha prestado libremente cuando: 1) no se permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto; o 2) cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.

Para evaluar si el consentimiento se ha prestado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato (art. 7.4 RGPD)⁸³. Sin embargo, debe tenerse en cuenta que, con carácter previo, deberá valorarse si el consentimiento se ha prestado válidamente de acuerdo a las normas generales de nuestro ordenamiento. En tal sentido, deberá prestarse por quien tenga capacidad para hacerlo (arts. 1.263 y 1.264 CC) y, de acuerdo con el art. 1.265 CC, además deberá emitirse libre de vicios, esto es, no podrá estar afectado por error, violencia, intimidación o dolo. De ahí que un consentimiento afectado por alguno de estos vicios impedirá el examen posterior del carácter libre, específico, informado e inequívoco conforme al RGPD.

80 STJUE de 11 de noviembre de 2020, Asunto C-61/19, caso *Orange România* (ECLI:EU:C:2020:901).

81 Más allá de este supuesto, que será el caso típico en el ámbito del suministro de contenidos y servicios digitales, como acertadamente señala GARCÍA-RIPOLL MONTIJANO, M.: “El consentimiento al tratamiento de datos personales”, en AA.VV.: *Protección de Datos Personales* (coord. por I. GONZÁLEZ PACANOWSKA), Tirant lo Blanch, Valencia, 2020, p. 119, los supuestos más claros de ausencia de libertad en el consentimiento son la violencia y la intimidación recogidas en el art. 1.267 CC.

82 MORALES BARCELÓ, J.: “El consentimiento del interesado en materia de protección de Datos del Reglamento UE 2016/679”, en AA.VV.: *El mercado Digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, Madrid, 2019, p. 309.

83 Vid., en el mismo sentido, el art. 6.3 LOPDGDD.

2. Consentimiento específico.

El art. 6.1, letra a) RGPD señala que el tratamiento será lícito si cumple, al menos, alguna de las condiciones establecidas en el citado precepto, entre las que se encuentra la siguiente: que el interesado haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. En este sentido, para que el consentimiento pueda considerarse válido es necesario que también sea específico conforme a la finalidad del tratamiento, la cual debe describirse de forma clara y en términos inequívocos.

Así, en lo que refiere a la nota de especificidad, el TJUE afirma⁸⁴ que la declaración debe presentarse de forma inteligible y de fácil acceso utilizando un lenguaje sencillo y claro, especialmente cuando se trate de un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento de datos personales. A este respecto, si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos (art. 7.2 RGPD)⁸⁵. Esto es, la manifestación de voluntad del interesado debe tener por objeto el tratamiento de datos específico de que se trate, no siendo correcto que ésta se deduzca de una manifestación de voluntad que tenga un objeto distinto. Además, conviene tener en cuenta que la especificidad de la libre voluntad obligará a obtener un nuevo consentimiento si los fines originarios cambian o se presenta un fin adicional⁸⁶.

3. Consentimiento informado.

Es evidente que para consentir adecuadamente hay que conocer aquello que se consiente⁸⁷. Por ello, tiene sentido que el art. 4.11 RGPD señale que el consentimiento del interesado equivale a una manifestación de voluntad “informada”⁸⁸. Por tanto, el consentimiento informado implica que el interesado debe conocer suficiente información antes de ejercer su opción. En tal sentido,

84 SSTJUE de 1 de octubre de 2019, Asunto C-673/17, caso Planet 49 (ECLI:EU:C:2019:801), y 11 de noviembre de 2020, Asunto C-61/19, caso Orange România (ECLI:EU:C:2020:901).

85 En este sentido, apunta el Cdo. 32 RGPD, el cual 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”. De la misma forma, el art. 6.2 LOPDGDD afirma que “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 embargo, como matiza ABA CATORIA, A.: “Principios de protección de datos”, en AA.VV.: *Comentarios a la Nueva Ley de Protección de Datos* (coord. por A. TURNES VILLANUEVA), Dilex, Madrid, 2020, p. 34, si hubiera vinculación entre los diversos fines podrían agruparse.

86 Vid., en este sentido, VÁZQUEZ-PASTOR JIMÉNEZ, L.: *Contratos de suministro de contenidos y servicios digitales*, Dykinson, Madrid, 2023, p. 71; y ABA CATORIA, A.: “Principios de protección”, cit., p. 35.

87 El Cdo. 39 RGPD señala expresamente que “Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados”.

88 GARCÍA-RIPOLL MONTIJANO, M.: “El consentimiento al tratamiento”, cit., p. 108.

para que el consentimiento sea informado, el interesado deberá conocer, como mínimo, la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales, pero, en su caso, también deberá estar informado de otras categorías tales como el plazo durante el cual se conservarán sus datos personales, la existencia de los derechos de acceso, rectificación o supresión, así como el derecho a oponerse al tratamiento, a la portabilidad de sus datos o, al ya mencionado, derecho a retirar el consentimiento en cualquier momento. Este consentimiento informado está relacionado con la especificidad a la que se ha hecho referencia en el apartado anterior, ya que el interesado solamente puede prestar su consentimiento para uno o varios fines específicos cuando está verdaderamente informado.

En las referidas sentencias⁸⁹, el TJUE, en relación con el carácter informado del consentimiento, establece que “el responsable del tratamiento facilitará al interesado información respecto de todas las circunstancias relacionadas con el tratamiento de datos, con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, debiendo el interesado conocer, en particular, qué datos serán tratados, la identidad del responsable del tratamiento, la duración del tratamiento y su forma, y los fines que se persigue con dicho tratamiento”. En la misma línea se pronuncia el Tribunal Constitucional⁹⁰, el cual señala que “el deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de la necesidad de consentimiento del afectado (...), pues si no se conoce su finalidad y destinatarios, difícilmente puede prestarse el consentimiento”.

Es importante también destacar la calidad de la información en el sentido de que la información suministrada por el responsable del tratamiento se debe adaptar al nivel de entendimiento de sus posibles destinatarios, esto es, que un usuario medio lo pueda entender sin mayores complicaciones⁹¹. En consecuencia, se debe permitir al interesado determinar fácilmente las consecuencias de su consentimiento y, en este sentido, que pueda dar y garantizar que dicho consentimiento se otorga con pleno conocimiento de causa.

Por su parte, el Cdo. 32 RGPD, si bien señala que es posible prestar el consentimiento mediante la marcación de una casilla de un sitio web en internet, excluye que el consentimiento haya sido prestado válidamente en aquellos casos

89 SSTJUE de 1 de octubre de 2019, Asunto C-673/17, caso Planet 49 (ECLI:EU:C:2019:801), y 11 de noviembre de 2020, Asunto C-61/19, caso Orange România (ECLI:EU:C:2020:901).

90 STC (Pleno) 39/2016, de 3 de marzo de 2016 (núm. 39/2016, 8 de abril de 2016) (ECLI:ES:TC:2016:39).

91 En tal sentido, VÁZQUEZ-PASTOR JIMÉNEZ, L.: *Contratos de suministro*, cit., p. 74, manifiesta que los responsables del tratamiento deben asegurarse que utilizan un lenguaje claro y sencillo en todos los casos, es decir, el mensaje debe ser comprensible para un ciudadano medio y no únicamente para juristas. Los responsables del tratamiento no pueden utilizar políticas de privacidad muy extensas que sean difíciles de entender o declaraciones llenas de jerga jurídica.

en que las casillas ya vienen marcadas por defecto. En este sentido, el TJUE⁹² ha declarado que “parece prácticamente imposible determinar de manera objetiva si el usuario de un sitio de Internet ha dado efectivamente su consentimiento para el tratamiento de sus datos personales al no quitar la marca de una casilla marcada por defecto y si dicho consentimiento ha sido dado, en todo caso, de manera informada. En efecto, no puede descartarse que dicho usuario no haya leído la información que acompaña a la casilla marcada por defecto, o que ni tan siquiera la haya visto, antes de proseguir con su actividad en el sitio de Internet que visita”.

Además, el TJUE⁹³ afirma que “para garantizar al interesado una verdadera libertad de elección, las estipulaciones contractuales no deben inducir al interesado a error en lo que respecta a la posibilidad de celebrar el contrato pese a negarse a dar su consentimiento para el tratamiento de sus datos”. En caso contrario –ante la ausencia de tal información-, no puede considerarse que el consentimiento del interesado al tratamiento de sus datos personales haya sido prestado libremente ni que, por otra parte, haya sido dado de manera informada.

4. Consentimiento inequívoco.

Según el art. 4.11 RGPD, el consentimiento debe ser inequívoco, es decir, debe existir una clara manifestación de voluntad por parte del interesado de que acepta el tratamiento de los datos. De esta forma, no deben existir dudas acerca de que el interesado está conforme en prestar su consentimiento para el tratamiento de sus datos. El carácter inequívoco implica, además, que debe ser el responsable del tratamiento de los datos el que ha de demostrar que el interesado ha prestado el consentimiento para el tratamiento de sus datos personales a través de un comportamiento activo. Esto es, la carga de la prueba relativa a la existencia de un consentimiento inequívoco incumbe al responsable del tratamiento, el cual debe ser capaz de demostrar esa licitud: que el interesado consintió en el tratamiento de sus datos personales.

El Cdo. 32 RGPD señala que este consentimiento inequívoco se puede prestar a través de una declaración por escrito -incluso por medios electrónicos- o a través de una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. En este sentido, de acuerdo con el art. 7.1 RGPD “Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales”,

92 STJUE de 11 de noviembre de 2020, Asunto C-61/19, caso *Orange România* (ECLI:EU:C:2020:901).

93 STJUE de 11 de noviembre de 2020, Asunto C-61/19, caso *Orange România* (ECLI:EU:C:2020:901).

lo cual está íntimamente ligado con el principio de responsabilidad proactiva que implica, conforme al art. 5.2 RGPD, que el responsable del tratamiento será responsable de que los datos sean tratados de manera lícita, leal y transparente en relación con el interesado⁹⁴. En consecuencia, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento (art. 24.1 RGPD).

VI. ¿CUÁNDO Y CÓMO SE TIENEN QUE CEDER LOS DATOS PERSONALES POR PARTE DEL CONSUMIDOR?

En los contratos de suministro de contenidos y servicios digitales, cuando la contraprestación consiste en la cesión de uso de los datos personales por parte del consumidor o usuario, otra de las cuestiones que surge es el momento y la forma en que dichos datos deben ser cedidos al empresario.

En primer lugar, respecto al momento en que los datos personales deben ser facilitados al empresario, el Cdo. 24 DCSD dispone que “Los datos personales podrían facilitarse al empresario en el momento en que se celebre el contrato o en un momento posterior; por ejemplo cuando el consumidor dé su consentimiento para que el empresario utilice los datos personales que el consumidor pueda cargar o crear con el uso de los contenidos o servicios digitales (...)”. De la misma forma, puede entenderse que los datos personales se pueden facilitar en el momento de celebración del contrato o en un momento posterior cuando el art. 59.4 TRLGDCU señala que el consumidor o usuario “facilita o se compromete a facilitar datos personales (...)”⁹⁵. De esto claramente se deduce que, en realidad, el momento en que el consumidor deba ceder o el empresario recabar los datos personales del consumidor o usuario dependerá de lo estipulado entre las partes en el contrato. No obstante, en este tipo de contratos, lo habitual es que no exista una negociación entre las partes respecto al momento de cesión de uso de los datos, sino que lo más frecuente es que nos encontremos ante condiciones predispuestas por el empresario a las que el consumidor deba adherirse.

En lo que respecta a la forma en que el empresario accede a los datos personales del consumidor cabe distinguir dos supuestos:

1) Por un lado, existen aquellos supuestos en que es el propio consumidor el que proporciona al empresario sus datos personales como, por ejemplo, aquellos casos en los que el consumidor, cuando utiliza ciertas aplicaciones o

⁹⁴ Vid. en este sentido, ABA CATOIRA, A.: “Principios de protección de datos”, cit., p. 32.

⁹⁵ Vid., en el mismo sentido, art. 3.1, párrafo 2° DCSD.

accede a determinados contenidos o servicios digitales, se registra previamente proporcionando así sus datos personales⁹⁶;

2) Por otro lado, nos encontramos con aquellos supuestos en los que no es el consumidor el que proporciona activamente los datos personales, sino que es el propio empresario el que obtiene por sí mismo los datos personales del consumidor o usuario⁹⁷. Lo cierto es que ni el TRLGDCU ni la DCSD, a diferencia de la PropDCSD⁹⁸, hacen referencia alguna a que sea obligatorio que los datos personales deban suministrarse a través de un comportamiento activo por parte del consumidor, por lo que no existen motivos para excluir la posibilidad de que sea el propio empresario quien recabe directamente, por sí mismo, los datos personales del consumidor o usuario. De hecho, consideramos que esta decisión es totalmente un acierto del legislador, pues si la única posibilidad que existiese fuera que los datos personales se suministraran activamente por parte del consumidor o usuario, esto podría suponer un incentivo para que los proveedores de contenidos y servicios digitales recabaran los datos personales por sí mismos, dejando estos supuestos fuera del ámbito de aplicación de la DCSD y del TRLGDCU y, en consecuencia, dejar al consumidor o usuario desprovisto de las medidas correctoras que estos textos normativos ofrecen⁹⁹. Por ello, nos parece conveniente acoger la posibilidad de que el empresario recabe los datos personales del consumidor o usuario a través de las denominadas *cookies*¹⁰⁰, posibilidad que estaba vetada en la

96 El Cdo. 24 DCSD señala que “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”, así como 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.”

97 El acceso a los datos personales de los individuos se puede llevar a cabo de formas muy diversas y a través de mecanismos muy heterogéneos. Por ejemplo, como indica ARTIGOT GOLOBARDES, M.: “La contratación digital con consumidores”, cit., p. 463, existen mecanismos para conocer el historial de navegación del individuo – a través de *cookies*-, para identificar su lugar de conexión – a través de las direcciones IP-, para realizar un seguimiento de los dispositivos –a través de las llamadas *device fingerprints*-, para obtener información personal a través de las llamadas *pixel tags* (pixels identificadores que se cargan cuando un individuo visita una página web o abre un correo electrónico), o a través de identificadores publicitarios (identificadores proporcionados por *Google Play* para monetizar las aplicaciones de manera más efectiva).

98 Concretamente, el Cdo. 14 de la PropDCSD señalaba que “En relación con los contenidos digitales no suministrados a cambio de un precio sino por otra contraprestación diferente al dinero, la presente Directiva debe aplicarse solo a los contratos en los que el proveedor solicita y el consumidor facilita datos de forma activa, como el nombre y la dirección de correo electrónico o fotos, directamente al proveedor, por ejemplo mediante el registro individual o sobre la base de un contrato que permite el acceso a las fotos del consumidor (...).” De esta forma, se exigía, en todo caso, una conducta activa por parte del consumidor o usuario, descartando cualquier otra forma en la que fuera el empresario quien recabara los datos personales por sí mismo.

99 *Vid.*, al respecto, arts. 117 y ss. TRLGDCU y arts. 13 y 14 DCSD.

100 Como señala MENÉNDEZ, L.: “¿Qué son las *cookies*?”, *Escritura pública*, núm. 82, 2013, p. 16, las *cookies* son “ficheros que se descargan en ordenadores, en teléfonos móviles o en tabletas al acceder a determinadas páginas web y permiten, entre otras cosas, almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo”. A su vez, NAVAS NAVARRO, S.: “*Cookies* y tecnología análoga: publicidad comportamental online y protección de los datos de carácter personal”, en AA.VV.: *Mercado digital: principios y reglas jurídicas* (dir. por S. NAVAS NAVARRO y S. CAMACHO CLAVIJO), Tirant lo Blanch, Valencia, 2016, p. 341, indica que “La *cookie* es un texto alfanumérico que se descarga en el equipo terminal del destinatario de la prestación de un servicio de la sociedad de la información cuya función es almacenar

PropDCSD, pero a la que en la versión definitiva de la DCSD y en el TRLGDCU no se ha hecho referencia, por lo que entendemos que el legislador ha querido dejar la puerta abierta a la posibilidad de que el empresario recabe también de esta forma los datos personales del consumidor¹⁰¹.

Con todo, si bien es cierto que la DCSD no excluye la posibilidad de que sus disposiciones se apliquen cuando el empresario recaba por sí mismo los datos personales del consumidor o usuario, su aplicación quedará supeditada a que la recopilación de tales datos personales por el empresario tenga la consideración de contrato en el derecho nacional, pues la DCSD únicamente es aplicable en la medida en que exista una relación contractual válida entre el empresario y el consumidor¹⁰². De esta forma, habrá que acudir al derecho nacional de los Estados miembros para determinar si estamos ante un contrato, dado que la propia DCSD no incorpora ninguna definición del mismo¹⁰³ ni establece reglas sobre celebración, validez, nulidad o efectos de los contratos¹⁰⁴, y así lo exige el Cdo. 25 DCSD donde se establece que para que la propia DCSD se aplique será necesario que la situación “se considere un contrato con arreglo al Derecho nacional”¹⁰⁵.

datos en el mismo que pueden ser recuperados por el prestador del servicio cuando el destinatario vuelve a solicitar la información, esto es, vuelva a conectar con el sitio web o con otro que forma parte de la misma red”. Por su parte, CABALLERO TRENADO, L.: “Cookies y consentimiento”, *Revista Crítica de Derecho Inmobiliario*, núm. 96, 2020, p. 3228, precisa que debido a que todos disponemos de dispositivos personales (smartphones, tablets y ordenadores personales) y a que estos están registrados e identificados de manera única, la información y datos que se generan cuando nos conectamos a Internet permite individualizar los datos y generar perfiles de usuarios y sus hábitos entrando en el terreno de los datos personales. Por todo ello, las cookies y otras tecnologías asimilables recopilan y tratan datos personales, y están sujetas al RGPD. Sin embargo, ALIÑO SEHWERT, J.J.: “La protección del consumidor digital: los datos personales en el comercio electrónico”, *Revista Jurídica sobre Consumidores y Usuarios*, núm. 3, 2018, p. 4, advierte que, si bien las “cookies” permiten al usuario una navegación ágil y personalizada, ello puede conllevar la pérdida de la privacidad de los datos con el fin de configurar un perfil del usuario para que la publicidad que se le muestre sea más acertada o subjetiva. De esta forma, las empresas pueden conocer muchos datos de los usuarios a través de los dispositivos, pero que, muchas veces, el consumidor ni siquiera es consciente de lo que está facilitando y, por ello, es preciso informar y contar con el consentimiento del usuario antes de su instalación. Para conocer los diferentes tipos de cookies y sus diferentes usos, *vid.*, a este respecto, GAROFALO, A.M.: “Cookies and the Passive Role of the Data Subject”, en AA.VV.: *Privacy and Data Protection in Software Services* (coord. por R. SENIGAGLIA, C. IRTI y A. BERNES), Signapur, 2022, pp. 73-76.

- 101 A los datos personales que se recogen y almacenan por el empresario a través de las cookies se les denomina “clickstream data” los cuales, como señala NAVAS NAVARRO, S. “El internet de las cosas”, *cit.*, pp. 34-35, son tratados, posteriormente, con diversas finalidades, entre ellas, la más frecuente es el envío posterior de publicidad “dirigida” online a ese destinatario a partir de un determinado perfil del mismo extraído sobre la base de la información que la cookie ha permitido tratar a su titular. El “clickstream data” contiene información básica como el tipo de ordenador que maneja el usuario para acceder a internet, el tipo de navegador o la identificación de cada sitio web que visita el usuario.
- 102 MILÀ RAFEL, R.: “Datos personales como contraprestación en la Directiva de contenidos y servicios digitales”, en AA.VV.: *Estudios de Derecho Contractual Europeo: nuevos problemas, nuevas reglas* (dir. por F. GÓMEZ POMAR e I. FERNÁNDEZ CHACÓN), Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2022, p. 425
- 103 A diferencia de la PropDCSD donde sí se incluía una definición de contrato en su art. 2.7, conforme al cual se entiende por “contrato” el “acuerdo que genera obligaciones u otros efectos jurídicos”.
- 104 Art. 3.10 y Cdo. 12 DCSD.
- 105 Sin embargo, nos sumamos a la opinión de ROSELLÓ RUBERT, F.M.: “Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales”, *Revista de Derecho Mercantil*, núm. 303, 2017, p. 13, quien defiende que hubiera sido deseable que el legislador europeo hubiese aunado bajo una única norma armonizadora todos los contratos de contenidos y servicios digitales a cambio de contraprestación no dineraria, ya que la diferencia entre aquellos cuyos datos personales se facilitan activamente y aquellos otros donde los datos se recaban mediante cookies no es tan sustancial. Con ello,

Por lo que respecta al ordenamiento jurídico español, como ya hemos avanzado, el TRLGDCU no veta esta posibilidad. De hecho, el art. 59.4 reconoce la aplicación del Libro II “Contratos y garantías” a “los contratos en virtud de los cuales el empresario suministra o se compromete a suministrar contenidos o servicios digitales al consumidor o usuario y este facilita o se compromete a facilitar datos personales”. Este precepto ha sido una transcripción literal del art. 3.1, párrafo 2º DCSD, lo que puesto en relación con la parte expositiva de la DCSD, donde el legislador europeo quiso eliminar la prohibición de que los datos personales se recabaran a través de *cookies*, unido a que el TRLGDCU tampoco lo prohíbe, debemos interpretar que el suministro de contenidos o servicios digitales a cambio de datos personales del consumidor, ya se recaben de forma activa o de forma pasiva, entrará dentro del ámbito de aplicación del Libro II TRLGDCU; y, de la misma forma ocurrirá en los demás Estados miembros, con excepción de aquellos que establezcan una disposición en la que se exija expresamente que se deben facilitar por parte del consumidor de forma activa o, en su caso, se vete al empresario la posibilidad de recabarlos directamente.

VII. SUPUESTOS EN QUE LOS DATOS PERSONALES NO CONSTITUYEN LA CONTRAPRESTACIÓN DEL CONTRATO.

Existen dos supuestos en los que la cesión de datos personales al empresario por parte del consumidor o usuario no constituye contraprestación del contrato.

En primer lugar, según el art. 59.4 TRLGDCU, encontramos aquellos casos en los que “los datos personales facilitados por el consumidor o usuario sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales”¹⁰⁶. De la misma forma, el Cdo. 25 DCSD señala que “la presente Directiva no debe aplicarse a las situaciones en las que el empresario recabe datos personales exclusivamente para suministrar contenidos o servicios digitales”. Por tanto, no tendrán la consideración de contraprestación contractual aquellos datos personales facilitados por el consumidor o usuario que sean necesarios para cumplir un requisito técnico, esto es, cuando sean necesarios para que el empresario pueda suministrar el contenido o servicio digital y, en consecuencia, pueda cumplir adecuadamente el contrato. Por ejemplo, en aquellos casos en que es necesario recabar datos sobre la localización geográfica para el adecuado funcionamiento de una App como *Google Maps*¹⁰⁷.

desde nuestra perspectiva, consideramos que se hubiese contribuido a la configuración de un régimen más armonizado y protector de los intereses del consumidor, ya que de esta forma la aplicación del régimen de conformidad a aquellos supuestos en que los datos se recopilen a través de *cookies* dependerá de cada ordenamiento nacional.

¹⁰⁶ Vid., en el mismo sentido, art. 3.1, párrafo 2º DCSD.

¹⁰⁷ No obstante, si los datos sobre la localización geográfica se utilizan, posteriormente, para fines distintos de los necesarios para cumplir con el requisito técnico, entonces sí que serán de aplicación la DCSD y el

Y, en segundo lugar, en virtud del mismo art. 59.4 TRLGDCU, encontramos aquellos supuestos en que los datos se recaban “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”. Al igual que en el caso anterior, el Cdo. 25 DCSD también señala que “la presente Directiva no debe aplicarse a las situaciones en las que el empresario recabe datos personales (...) con el único fin de cumplir requisitos legales”. De ahí que cuando la cesión de datos personales al empresario por parte del consumidor o usuario tenga por objeto el cumplimiento de las prescripciones legales, esos datos no tendrán naturaleza de contraprestación contractual. Sería el caso, por ejemplo, de aquellos supuestos en los que el registro del consumidor fuera necesario en virtud de la legislación aplicable por motivos de seguridad e identificación.

Estas dos exclusiones que acabamos de ver responden a un doble fundamento¹⁰⁸:

Por un lado, el empresario, en estos casos, no suministra los contenidos o servicios digitales a cambio de datos personales (entendidos como contraprestación contractual), sino que únicamente recaba los datos para cumplir con unos requisitos, ya sean requisitos técnicos o requisitos legales. El empresario, en estos supuestos, obtendrá el beneficio a través de otras vías como, por ejemplo, el pago de un precio en dinero, pero no a través de los datos personales del consumidor o usuario, cuya obtención responde únicamente a finalidades técnicas o legales.

Por otro lado, íntimamente ligado a lo anterior, el tratamiento que el empresario pueda realizar sobre los datos personales cedidos por el consumidor o usuario será lícito de acuerdo con el art. 6.1 RGPD, pero no con base en el consentimiento del titular de los datos del apartado a) de dicho precepto, sino en cumplimiento de los apartados b) y c) del referido artículo. Es decir, el tratamiento de los datos personales será lícito cuando el tratamiento sea “necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales”, así como cuando el tratamiento sea “necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”. Por tanto, si los datos personales del consumidor son recabados para cumplir con una finalidad técnica o legal, el consentimiento para el tratamiento de esos datos personales no deberá recogerse sobre la base del apartado a) del art. 6.1 RGPD, sino que la licitud del consentimiento estará sometida a su obtención de acuerdo con las previsiones de los apartados b) y c) del art. 6.1 RGPD.

En definitiva, es importante señalar que para que la cesión de datos personales por parte del consumidor y usuario no sea considerada como contraprestación

TRLGDCU.

108 Vid., en este sentido, MARTÍNEZ CALVO, J.: “Los datos personales”, cit., p. 104.

del contrato es necesario que únicamente sean tratados para finalidades técnicas o legales, tal y como establecen los arts. 3.1, párrafo 2º DCSD y 59.4 TRLGDCU, pues, en caso contrario, deberá reconocerse su naturaleza de contraprestación contractual, especialmente cuando los mismos sean tratados para fines comerciales¹⁰⁹. En este sentido, si los datos personales se consideran contraprestación del contrato serán de aplicación las previsiones de la DCSD y el TRLGDCU. No obstante, si opera alguna de las exclusiones a las que nos hemos referido –técnicas o legales- la consecuencia será que no resultarán de aplicación los mecanismos de protección previstos en la DCSD y el TRLGDCU¹¹⁰, lo que implica que el nivel de protección del consumidor o usuario sea menor que en aquellos casos en los que sí exista contraprestación, independientemente de que ésta consista en el pago de un precio en dinero o en la cesión de datos personales para fines distintos de los previstos.

Por último, el Cdo. 25 DCSD señala que la Directiva “tampoco debe aplicarse a situaciones en las que el empresario recaba únicamente metadatos tales como información sobre el dispositivo del consumidor o el historial de navegación”¹¹¹, así como a aquellas “situaciones en las que el consumidor, sin haber celebrado un contrato con el empresario, se expone a recibir publicidad con el fin exclusivo de obtener acceso a contenidos o servicios digitales”¹¹². No obstante, si bien es cierto que estas situaciones están excluidas del ámbito de aplicación de la DCSD¹¹³, el propio Cdo. 25 otorga libertad a los Estados Miembros para que puedan aplicar la

109 Tal y como señala HERRERÍAS CASTRO, L.: “Contratos de suministro de contenidos y servicios digitales: cuando el precio son tus datos personales”, *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, p. 1019, ambas exclusiones estarían justificadas porque el empresario no obtiene ningún beneficio económico derivado del tratamiento de los datos personales de los consumidores.

110 En tal sentido, como apunta SENÉCHAL, J.: “Article 16(2) of the ‘Digital Content and Digital Services’ Directive on the Consequences of Termination of Contract, or the Difficult Articulation between Union Law on Consumer Contract and Union Law on the Protection of Personal Data”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSE, R. SCHULZE y D. STAUDEMANYER) Nomos/Hart, Baden-Baden (Munich), 2020, p. 156, la Directiva únicamente se aplicará a los contratos de suministro de contenidos o servicios digitales de carácter sinalagmático u oneroso, pero no de aquellos genuinamente gratuitos. Esto es, se aplicará cuando los datos personales constituyan la contraprestación del contrato, lo que no ocurrirá cuando los mismos se faciliten para cumplir con las cuestiones meramente técnicas o legales; al respecto, MARTÍNEZ CALVO, J.: “Los datos personales”, cit., p. 104, considera que, cuando los contenidos o servicios digitales se suministran al consumidor sin contraprestación alguna por parte de este, resulta razonable que el nivel de protección que otorga la normativa sea menor que en aquellos supuestos en los que el consumidor ha de llevar a cabo una contraprestación, ya sea dineraria o no dineraria. Por el contrario, PLANA ARNALDOS, M.C.: “Los datos personales como contraprestación”, cit., p. 590, se muestra crítica con esta decisión del legislador de excluir la aplicación de la DCSD en estos casos en que los datos son tratados para cumplir requisitos legales, ya que considera que en los casos en que el contrato no fuese finalmente conforme, el consumidor debería poder utilizar el derecho a resolver, con la consecuente obligación del proveedor de abstenerse de utilizar los datos.

111 Los metadatos son, como señala CÁMARA LAPUENTE, S.: “Resolución contractual y destino de los datos y contenidos generados por los usuarios de servicios digitales”, *Cuadernos de Derecho Transnacional*, vol. 12, núm. 1, 2020, p. 850, nota 38. “etiquetas o datos anexados a archivos de todo tipo que contienen palabras clave, información sobre autoría, modificaciones, etc., generados automáticamente o de creación humana que sirven sobre todo para la catalogación de los archivos (imágenes, vídeos, páginas, documentos, etc.) en índices y su recuperación en la web semántica”.

112 Por ejemplo, el anuncio publicitario que debe soportar el usuario antes de ver un vídeo en *Youtube*.

113 CÁMARA LAPUENTE, S.: “Una perspectiva crítica sobre el régimen de los contratos de suministro de contenidos digitales”, en AA.VV.: *Derecho digital: retos y cuestiones actuales* (dir. por F. CAPILLA RONCERO,

DCSD a tales situaciones o de regular tales situaciones. Sin embargo, el legislador español, al transponer la DCSD al TRLGDCU, no ha aclarado esta cuestión. Es decir, no ha aclarado si algunas prácticas de navegación por internet constituyen o no contratos a los efectos de la normativa de protección del consumo, tales como acceder a prensa digital o a páginas web sin registro previo cuando lo que se recaba son, únicamente, los metadatos a los que acabamos de hacer referencia o, simplemente, el consumidor se expone a recibir publicidad con el fin exclusivo de obtener acceso a determinados contenidos o servicios digitales.

Dado que se trataba de una posibilidad que tenían los Estados miembros de ampliar el ámbito de aplicación de la DCSD a estos supuestos que, en principio, estaban excluidos, el silencio del Real Decreto Ley 7/2021, que no se ha pronunciado al respecto, nos lleva a plantearse la cuestión de si el TRLGDCU podría aplicarse a este tipo de situaciones. En tal sentido, como señala parte de la doctrina más autorizada¹¹⁴, estas situaciones no hay que entenderlas como necesariamente excluidas, si, a la luz de las reglas del Código civil y del Derecho común de obligaciones y contratos, puede entenderse que en el ordenamiento español merecen tal calificación contractual¹¹⁵. De ahí que a efectos de aplicación de la norma, lo que habrá que determinar es si se ha celebrado o no un contrato conforme al Derecho nacional.

A nuestro entender, es un error por parte del legislador europeo dejar en manos de los Estados miembros la calificación o no como contratos de este tipo de situaciones, ya que ello supone una falta de armonización entre los diferentes ordenamientos¹¹⁶, lo cual va en contra de los objetivos de la propia DCSD, tales como proporcionar un régimen unificado y acabar con la inseguridad jurídica. Ahora bien, cabe la posibilidad de que esta situación se solucione y se logre una mayor armonización entre legislaciones nacionales mediante la revisión de la DCSD, la cual ya debería haberse realizado, pues estaba prevista, a más tardar, para el 12 de junio de 2024, pero, la realidad es que aún no se ha llevado a cabo. Cuando tenga lugar, la Comisión deberá presentar un informe de revisión, en el cual se examinarán, entre otras cuestiones, la armonización de las normas aplicables a los contratos de suministro de contenidos y servicios digitales distintos a los previstos por la DCSD, incluidos los suministrados a cambio de anuncios publicitarios¹¹⁷.

et.al.), Thomson Reuters - Aranzadi, Cizur Menor (Navarra), 2018, p. 53 señala que esta exclusión carece de un fundamento sólido.

114 CÁMARA LAPUENTE, S.: "Un primer balance de las novedades del RDL 7/2021, de 27 de abril, para la defensa de los consumidores en el suministro de contenidos y servicios digitales", *Diario La Ley*, núm. 9887, 2021, p. 25.

115 Esta tesis es igualmente apoyada por HERRERÍAS CASTRO, L.: "Contratos de suministro", p. 1020.

116 También se muestran muy críticos con esta falta de armonización ROBERT, R. y SMIT, L.: "The proposal for a directive on digital content: a complex relationship with data protection law", *ERA Forum*, vol.19, núm. 2, 2018, p. 172.

117 Así lo dispone expresamente el art. 25 DCSD.

En cualquier caso, lo que sí parece claro es que algunos de los proveedores con más popularidad y relevancia en el mercado plantean desde un principio la oferta de contenidos y servicios digitales en términos contractuales. Así, por ejemplo, *Apple* en sus “términos y condiciones de los servicios de contenido multimedia” indica que “*Estos términos y condiciones crean un contrato entre tú y Apple (el “Contrato”)*”¹¹⁸. O, por ejemplo, *X* (el anteriormente conocido como *Twitter*), en cuyos “Términos de servicio” señala que “*Estos Términos de servicio (“Términos”) son parte del Acuerdo de usuario, un contrato legalmente vinculante que rige el uso de X*”¹¹⁹. También lo hace así *Youtube* en sus “Términos del servicio” donde se afirma que “*“Puedes acceder al Servicio y usarlo, tal cual se pone a tu disposición, siempre y cuando cumplas con lo establecido en este Contrato y en la ley”*”¹²⁰. Por tanto, en estos casos, el problema de la calificación parece estar resuelto.

Por último, cabe plantearse si resultaría de aplicación la DCSD y el TRLGDCU a aquellos supuestos en que el contrato de suministro de contenidos y servicios digitales exige el pago de un precio en dinero y, además, es necesario que el consumidor se exponga a publicidad para obtener acceso al contenido o servicio digital. En tales casos, consideramos, fuera de toda duda, que deberían aplicarse la DCSD y el TRLGDCU, pues claramente estamos ante un contrato, donde el pago de un precio con dinero ya determina la onerosidad del mismo, con independencia de lo que pudieran señalar, en su caso, los ordenamientos nacionales respecto a la otra parte de la contraprestación que consista en metadatos.

VIII. LAS BASES JURÍDICAS QUE PUEDEN LEGITIMAR EL TRATAMIENTO DE LOS DATOS PERSONALES CUANDO ESTOS SE UTILIZAN PARA FINES COMERCIALES.

Como ya hemos visto en el apartado precedente, cuando los datos personales del consumidor son tratados por cuestiones técnicas (con el fin de suministrar los contenidos o servicios digitales) o legales (con el fin de que el empresario cumpla sus obligaciones legales), la base que legitima ese tratamiento la encontramos en el art. 6 apartados b) y c) del RGPD, dado que esos datos son “necesarios para la ejecución de un contrato en el que el interesado es parte” o bien porque se basa en el “cumplimiento de una obligación legal aplicable al responsable”, que es el empresario.

118 Consultar en: <https://www.apple.com/legal/internet-services/itunes/es/terms.html> (fecha de consulta: 25 de octubre de 2024).

119 Consultar en: <https://x.com/es/tos> (fecha de consulta: 25 de octubre de 2024).

120 Consultar en: <https://www.youtube.com/static?template=terms&hl=es&gl=AR> (fecha de consulta: 25 de octubre de 2024).

No obstante, cuando los datos facilitados por el consumidor son tratados por el empresario para finalidades distintas al suministro de los contenidos y servicios digitales, especialmente cuando se tratan para fines comerciales, nos podemos plantear la posibilidad de que dicho tratamiento pueda encontrar justificación en diferentes causas de licitud, pues 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 art. 6.1 RGPD¹²¹. Además, conviene resaltar la importancia de determinar la base legal que sirve para el tratamiento antes de comenzar propiamente la actividad del tratamiento de los datos, dado que las bases en que se justifica dicho tratamiento no son intercambiables constante el tratamiento, toda vez que se deben incorporar al contenido obligatorio del deber de información¹²². Seguidamente vamos a analizar, en concreto, el tratamiento basado en la necesidad para la ejecución del contrato [art. 6.1, letra b) RGPD]; el tratamiento basado en el interés legítimo [art. 6.1, letra f) RGPD]; y el consentimiento del consumidor [art. 6.1, letra a) RGPD].

I. Tratamiento basado en la necesidad para la ejecución del contrato ex art. 6.1, letra b) RGPD.

En primer lugar, si consideramos que el contrato de suministro de contenidos y servicios digitales es un contrato bilateral en el que cada una de las partes asume una serie de obligaciones –en el caso del empresario suministrar los contenidos y servicios digitales y, en el caso del consumidor, ceder el uso de sus datos personales como contraprestación–, podemos plantearnos si los datos personales requeridos por el empresario son necesarios para la ejecución del contrato, incluso, a pesar de que se trate de datos que vayan a ser tratados para finalidades distintas al suministro de contenidos y servicios digitales, ya que si estos datos no se proporcionan, el contrato no se ejecuta, precisamente, porque actúan a modo de contraprestación.

Desde este planteamiento, si los datos facilitados por el consumidor o usuario, que van a ser tratados para finalidades distintas al suministro, los consideramos como “necesarios para la ejecución del contrato”, nos podría servir de base legitimadora el propio art. 6.1, letra b) RGPD¹²³. En este sentido, el propio consentimiento contractual legitimaría al proveedor para tratar los datos personales cedidos por el consumidor, no siendo necesario encontrar justificación legítima en el consentimiento del art. 6.1, letra a) RGPD. En consecuencia, este tratamiento de

121 GARCÍA PÉREZ, R.M.: “Interacción entre protección del consumidor y protección de datos personales en la Directiva (UE) 2019/770: licitud del tratamiento y conformidad de contenidos y servicios digitales”, en AA.VV.: *El derecho privado en el nuevo paradigma digital* (dir. por. E. ARROYO AMAYUELAS y S. CÁMARA LAPUENTE), Marcial Pons, Madrid, 2020, p. 181.

122 Vid., en este sentido, los arts. 13.1, letra c), 14.1, letra c) y 14.2, letra b) RGPD.

123 Esta es la postura que defiende MARTÍNEZ MARTÍNEZ, R.: “¿Consentimiento o contrato?” (Consultar en: <http://lopyseguridad.es/consentimiento-o-contrato/>).

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 preveyesen su revocación (a diferencia de la libre revocabilidad del tratamiento de datos basado en el consentimiento conforme al art. 7.3 RGPD)¹²⁴.

Ahora bien, este planteamiento en el que los datos personales se consideran “necesarios para la ejecución del contrato” por encontrarse ante la existencia de un contrato bilateral y que, por tanto, se constituyen como una obligación asumida por las partes que debe ser ejecutada, consideramos que no es adecuada, ya que el art. 6.1, letra b) RGPD –si lo interpretamos desde un punto de vista teleológico– no se refiere a la “necesidad” de los datos en este sentido, sino que se está refiriendo al supuesto en que los mismos son necesarios para el cumplimiento de requisitos técnicos¹²⁵. Por tanto, desde el momento en el que los datos personales cedidos por el consumidor son tratados para fines distintos del cumplimiento de requisitos técnicos del contrato, estos datos ya no deberían encontrar como base legítima el art. 6.1, letra b) RGPD. De hecho, así lo han entendido también las autoridades europeas en materia de protección de datos:

Por un lado, el Grupo de Trabajo del artículo 29 (GT29), ya 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*¹²⁶, de 9 de abril de 2014, hizo una interpretación de lo que debía suponer la disposición relativa a que el tratamiento sea “necesario para la ejecución de un contrato en el que el interesado sea parte”. En este sentido, consideró, que “Esta disposición debe interpretarse de manera estricta y no comprende situaciones en las que el tratamiento no sea realmente necesario para la ejecución de un contrato, sino unilateralmente

124 GARCÍA PÉREZ, R.M.: “Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales”, *Cuadernos de derecho transnacional*, vol. 12, núm. 1, 2020, p. 890. En un sentido similar se pronuncia NAVAS NAVARRO, S.: “Datos personales y mercado”, en AA.VV.: *Inteligencia artificial: tecnología, derecho* (dir. por. S. NAVAS NAVARRO), Tirant lo Blanch, Valencia, 2017, p. 266, quien explica que si los datos personales funcionan como contraprestación, el consentimiento dado por su titular es un consentimiento contractual, la finalidad o finalidades para la cual sus datos son tratados es un motivo causalizado y, si el consumidor retira su consentimiento, incumple, salvo que se hubiese pactado la facultad de desistimiento.

125 Vid., en este sentido, WENDEHORST, C.: “Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?*, (dir. por S. LOHSSE, R. SCHULZE y D. STAUDEMANYER), Nomos/Hart, Baden-Baden (Munich), 2020, p. 201; JANECEK, V. y MALGIERI, G.: “Data Extra Commercium”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSSE, R. SCHULZE y D. STAUDEMANYER), Nomos/Hart, Baden-Baden (Munich), 2020, cit. p. 112; ZOLL, F.: “Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content”, en AA.VV.: *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps* (dir. por R. SCHULZE, D. STAUDEMANYER y S. LOHSSE), Nomos/Hart, Baden-Baden (Munich), 2017, p. 183; MARTÍNEZ CALVO, J.: “Dualidad normativa en la regulación de los contratos gratuitos de suministro de contenidos y servicios digitales: la necesaria armonización entre la Directiva (UE) 2019/770 y el Reglamento (UE) 2016/679”, *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, p. 1175; y DOMÍNGUEZ YAMASAKI, M.I.: “El tratamiento de datos personales”, cit., pp. 106-107.

126 Consultar en: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

impuesto al interesado por parte del responsable del tratamiento¹²⁷. De ahí que, por ejemplo, el art. 6.1, letra b) RGPD no sirva como fundamento jurídico para elaborar un perfil de los gustos y las opciones de estilo de vida del usuario, basado en su recorrido por un sitio web y en los artículos adquiridos. Y, además, el GT29 consideró que debe existir una clara relación entre la “necesidad” y el principio de limitación de la finalidad¹²⁸, ya que la evaluación para comprobar si el tratamiento de datos es necesario para su ejecución se realizará en función de la información que se le haya dado previamente al interesado sobre el tratamiento de sus datos. Por ello, es importante justificar de forma exacta la esencia y objetivo fundamental del contrato.

Por otro lado, el Comité Europeo de Protección de Datos (CEPD) –que es la entidad que sustituye al GT29–, tras la aprobación del RGPD, publicó la *Guía 2/2019 para el tratamiento de datos personales conforme al artículo 6.1.b) en el contexto de los servicios en línea*¹²⁹ donde interpreta el concepto de “necesidad” en la misma línea en que ya lo hizo el GT29. En este sentido, el CEPD señala que cuando evaluamos qué se entiende por “necesario”, debe realizarse una valoración conjunta de los hechos del tratamiento, teniendo en cuenta el objetivo que se persigue y evaluando aquellas opciones que resulten menos intrusivas para conseguir el referido objetivo, de forma que si existen alternativas que sean posibles y menos intrusivas, se considerará que el tratamiento no es “necesario”. Además, añade que es necesario que el responsable pueda demostrar que el tratamiento tiene lugar en el contexto de un contrato válido con el interesado y que el tratamiento sea objetivamente necesario para la ejecución de dicho contrato. En consecuencia, el hecho de que se incluya en el contrato la expresión “necesario para la ejecución” como mera cláusula contractual no basta para considerar como base legítima para el tratamiento de los datos personales el referido art. 6.1, letra b) RGPD. Por su parte, el CEPD, finalmente, opta por ratificar la orientación adoptada por el GT29 sobre la disposición equivalente en virtud de la Directiva anterior –art. 7, letra b) Directiva 95/46/CE– a la que hemos hecho referencia anteriormente.

127 Vid., a este respecto, DE FRANCESCHI, A.: “Personal Data as Counter”, cit., p. 64, quien también aboga por una interpretación estricta del requisito de la “necesidad”, aunque advierte que, en estos casos, no está claro si la cantidad de datos necesarios para el cumplimiento del contrato debería determinarse subjetivamente (desde la perspectiva del empresario) u objetivamente.

128 El principio de limitación de la finalidad viene recogido en el art. 5.1, letra b) RGPD el cual señala que “Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (...)”. En palabras de APARICIO VAQUERO, J.P.: “Principios del tratamiento y derechos de los interesados en la nueva normativa de protección de datos personales”, *Rued@: Universidad Ética y Derechos*, núm. 3-4, 2019, p. 11, “Todo tratamiento debe tener una finalidad determinada (no caben expresiones genéricas), explícita (conocida, debe ser comunicada al interesado) y legítima (conforme con la normativa, ha de tener una base que lo legitime: consentimiento, norma, contrato...), no pudiendo ser usados los datos personales para otros fines incompatibles; es lo que se conoce como ‘limitación de la finalidad’”.

129 Consultar en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf

Por último, en esta misma Guía se indican una serie de casos¹³⁰, a modo ejemplificativo, uno de los cuales hace referencia a un comercio minorista que desea elaborar perfiles de los gustos y el estilo de vida de los usuarios en función de sus visitas al sitio web. Aclara que la ejecución del contrato de compraventa no depende de la elaboración de estos perfiles y, por tanto, aunque en el contrato se mencione específicamente y se informe al interesado de la elaboración de estos perfiles, esta elaboración no es "necesaria", de por sí, para la ejecución del contrato y, en consecuencia, si el minorista desea elaborar estos perfiles, deberá invocar un fundamento jurídico diferente a este art. 6.1, letra b) RGPD¹³¹. De ahí resulta claramente que cuando en los contratos de suministro de contenidos y servicios digitales, el empresario recabe los datos personales del consumidor o usuario para fines distintos de aquellos estrictamente necesarios para la ejecución del contrato, el art. 6.1, letra b) RGPD no podrá servir de base legítima para ello, especialmente, cuando los datos vayan a ser tratados para fines comerciales, como ocurrirá en la mayoría de casos.

2. Tratamiento basado en el interés legítimo ex art. 6.1, letra f) RGPD.

En segundo lugar, podríamos plantearnos si los datos personales que se recaban por el empresario en el marco de un contrato de suministro de contenidos y servicios digitales podrían encontrar justificación en la necesidad de satisfacer un interés legítimo del propio empresario (responsable del tratamiento) conforme al art. 6.1, letra f) RGPD¹³². Este interés legítimo encuentra su límite en los intereses o en los derechos y libertades fundamentales del interesado, debiendo ponderar en cada caso esta confrontación de intereses y derechos del responsable y del interesado¹³³, prevaleciendo, como es obvio, siempre los derechos y libertades fundamentales del titular de los datos, que será el consumidor que los ceda a cambio del suministro del contenido o servicio digital.

130 *Vid.*, en este sentido, Guía 2/2019 para el tratamiento de datos personales conforme al artículo 6.1.b) en el contexto de los servicios en línea, p. 12.

131 *Vid.*, en un sentido similar, AMMERMAN YEBRA, J.: "El alcance de las cláusulas contenidas en los contratos de suministro de contenidos y servicios digitales que prevén la interacción del usuario con el servicio mediante comandos de voz", *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, p. 1117, quien también considera que esta base legítima no es adecuada para el tratamiento de "datos de voz", en concreto, cuando se trata de asistentes de voz cuyo propósito es el reconocimiento de una determinada voz (la del usuario) y no otra, que es lo que se conoce como "reconocimientos de voz" a través de los cuales se crean modelos de voz y, por tanto, el tratamiento de la voz, como forma de identificación de la persona, queda claro en estos casos. En consecuencia, dado que se trata de un dato biométrico (dato personal de categoría especial) será necesario el consentimiento explícito del interesado ex art. 9.2, letra a) RGPD.

132 El art. 6.1, letra f) RGPD señala que el tratamiento será lícito cuando sea "necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

133 En este mismo sentido, MARTÍNEZ VILLASECA, M.: "El interés legítimo como base legitimadora del tratamiento de datos de carácter personal", *Actualidad administrativa*, núm. 12, 2019, p. 5, señala que se debe realizar el juicio de idoneidad y proporcionalidad entre la satisfacción de los intereses perseguidos por el responsable del tratamiento o por el tercero al que se comunicuen los datos y los derechos y libertades fundamentales de los interesados.

Este “interés legítimo” es un concepto indeterminado¹³⁴, pero que se basa en los motivos que tiene el responsable para recoger, almacenar o comunicar los datos personales ajenos a terceros. En este sentido, para que el tratamiento de datos personales ex art. 6.1, letra f) RGPD sea lícito debe reunir una serie de requisitos que se han ido perfilando por la jurisprudencia¹³⁵, a saber: 1) que exista un interés legítimo del responsable, conforme a derecho y respetuoso con las normas generales y sectoriales; 2) que se cumpla el principio de necesidad, esto es, que el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable; y 3) que el resultado de la ponderación entre el interés legítimo y los derechos e intereses del afectado que pudieran verse afectados por el tratamiento sea favorable para este último.

Además, para que un “interés legítimo” se considere adecuado y pertinente y, por ende, se pueda considerar relevante para poder fundar en el mismo el análisis de ponderación requerido por la norma, el GT29 en su Dictamen 6/2014¹³⁶ señala que el mismo debe ser específico (es decir, estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se lleve a cabo en contraposición a los intereses y los derechos fundamentales del interesado) y representar un interés real y actual (es decir, no especulativo).

El “interés legítimo” como base legitimadora podrá justificar el tratamiento de datos personales para determinadas finalidades (personalización de contenidos, prevención del fraude, envío de comunicaciones de carácter promocional, publicidad dirigida, presentación de ofertas relevantes, etc.)¹³⁷, 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

134 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, señala que “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”.

135 Vid., en este sentido, SSTJUE de 24 de noviembre de 2011, Asuntos C-468/10 y C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEDM) (ECLI:EU:C:2011:777), 13 de mayo de 2014, Asunto C131/12, Caso Google Spain S.L vs. Agencia Española de Protección de Datos (AEPD) (ECLI:EU:C:2014:317), 4 de mayo de 2017, Asunto C-13/16, Rigas Satskime (ECLI:EU:C:2017:336), y 29 de julio de 2019, Asunto C-40/17, Fashion ID GmbH & Co.KG vs. Verbraucherzentrale NRW eV (ECLI:EU:C:2019:629).

136 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, p. 30.

137 Vid., en este sentido, los Cdos. 47 a 49 RGPD donde se contemplan algunos supuestos que se consideran interés legítimo. Y, en esta misma línea, WENDEHORST, C.: “Personal Data in Data Value Chains”, cit., p. 202, afirma que la base jurídica de los intereses legítimos debe interpretarse de forma restrictiva, de manera que solamente quedarían cubiertos aquellos supuestos en los que el responsable del tratamiento usa los datos personales del interesado para fines mercadotécnicos de sus propios productos y servicios hacia sus propios clientes.

del interesado¹³⁸. Para ello, la ponderación de intereses a la que hemos hecho referencia debe ser favorable, es decir, el interés legítimo del responsable debe prevalecer por encima de los intereses, derechos y libertades fundamentales del interesado, lo que, desde luego, cuando los datos personales sean cedidos como contraprestación del suministro de contenidos y servicios digitales, no ocurrirá, pues el beneficio económico que pueda obtener el empresario con los datos personales del consumidor o usuario, desde nuestro punto de vista, no puede considerarse nunca un “interés legítimo” que prevalezca sobre los derechos y libertades del interesado-consumidor¹³⁹. De hecho, así lo ha reconocido también el TJUE¹⁴⁰, el cual ha afirmado que el derecho fundamental a la protección de datos –entre otros- prevalece, como regla general, sobre los intereses económicos del responsable del tratamiento.

Cuestión distinta es que los proveedores digitales recurran al “interés legítimo” como base de licitud de determinadas finalidades del tratamiento de datos personales, distintas a fines de comercialización. De hecho, una práctica frecuente es que los proveedores de contenidos y servicios digitales, en sus clausulados y políticas de privacidad¹⁴¹, recurran a este interés legítimo como causa legitimadora del tratamiento para finalidades tales como personalizar y mejorar los productos y servicios, facilitar vías de comunicación sin fines de comercialización, fomentar funciones de productos innovadores, mantener la seguridad de las plataformas y verificar las redes o para evitar e impedir casos de fraude o abusos, entre otros.

3. Consentimiento del consumidor ex art. 6.1, letra a) RGPD.

Por último, se plantea la posibilidad de que la base legitimadora para justificar el tratamiento de los datos personales del consumidor cedidos como contraprestación del contenido o servicio digital sea la establecida en el art. 6.1,

138 GARCÍA PÉREZ, R.M.: “Bases jurídicas relevantes”, cit., p. 899.

139 Vid., en el mismo sentido, FERNÁNDEZ CHACÓN, I.: “Caracterización y régimen aplicable”, cit., p. 242. Además, tal y como afirman JANECEK, V. y MALGIERI, G.: “Data Extra Commercium”, cit., p. 113, siempre se podría argumentar que el beneficio económico deseado podría lograrse mediante medios menos invasivos como, por ejemplo, mediante el ofrecimiento por parte de los proveedores de contenidos digitales de servicios “premium” a cambio del pago de un precio en dinero.

140 STJUE, de 13 de mayo de 2014, asunto C-131/12, Caso Google Spain S.L vs. Agencia Española de Protección de Datos (AEPD) (ECLI:EU:C:2014:317).

141 Como señala ALIÑO SEHWERT, J.J.: “La protección del consumidor digital”, cit., p. 5, “la política de privacidad de una empresa es el conjunto de principios que ha adoptado en relación con los datos personales que le han sido confiados, su finalidad, su seguridad, sus comunicaciones a terceros, la forma de canalizar el ejercicio de los derechos de los afectados, etc., siempre dentro del marco que permite la normativa en la materia”. Y añade que “la correcta aplicación de la política de privacidad debe comenzar con el cumplimiento de los requisitos legales para la lícita obtención de los datos personales”. Vid., en este sentido, los clausulados y políticas de privacidad de los principales proveedores de contenidos y servicios digitales como Facebook (<https://www.facebook.com/privacy/policy/>), Whatsapp (<https://www.whatsapp.com/legal/privacy-policy/?lang=es>), Twitter (<https://x.com/es/privacy>) Spotify (<https://www.spotify.com/es/legal/privacy-policy/>), Dropbox (https://www.dropbox.com/es_ES/privacy), Google (<https://policies.google.com/privacy?hl=es>) o Apple (<https://www.apple.com/legal/privacy/es/>).

letra a) RGPD, esto es, el consentimiento del interesado para el tratamiento de sus datos personales para uno o varios fines específicos.

Consideramos que esta opción es la más correcta, dado que el tratamiento de los datos personales del interesado para fines comerciales puede encontrar cabida bajo la expresión “para uno o varios fines específicos” establecida en este artículo y, en consecuencia, reconocerse la licitud del tratamiento siempre y cuando se cumplan los requisitos que dicho consentimiento exige ex art. 4.11 RGPD y 6.1 LOPDGDD, esto es, que se preste de forma libre, específica, informada e inequívoca¹⁴². Sobre todo, hay que tomar especial cautela con el requisito de la “especificidad” que se contiene en el propio art. 6.1, letra a) RGPD. Ello implica que el suministrador en la declaración de consentimiento deberá describir de forma clara e inequívoca la finalidad del tratamiento; y que, en el caso de que los datos vayan a ser tratados para varios fines, se debe requerir el consentimiento del interesado por separado para cada uno de estos fines¹⁴³. De hecho, es la propia DCSD en su Cdo. 38 la que hace referencia especialmente al consentimiento del art. 6.1, letra a) RGPD como base legítima para el tratamiento de datos personales, estableciendo que, en su caso, las condiciones para valorar si el consentimiento se presta libremente se regirán por las disposiciones del RGPD.

142 *Vid., supra* apartado 5.

143 Si se analizan las políticas de privacidad de los proveedores de contenidos y servicios digitales más importantes, se puede comprobar cómo la base legitimadora del consentimiento es utilizada de forma diferente por cada uno de ellos. Así, por ejemplo, Facebook (https://www.facebook.com/about/privacy/legal_bases) indica que la base jurídica del consentimiento se emplea: 1) “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”; 2) “Para usar los datos que los anunciantes y otros socios nos proporcionen sobre tu actividad fuera de los Productos de las empresas de Meta, 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”; 3) “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”; 4) “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”.

Por su parte, Google (<https://policies.google.com/privacy?hl=es>) también hace referencia al consentimiento para compartir “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”.

En cambio, Apple (<https://www.apple.com/legal/privacy/es/>) establece una declaración genérica en la que no concreta la base jurídica que legitima su tratamiento de datos, pues simplemente expone las diferentes posibilidades en las que puede basarse en función de las circunstancias, remitiéndose, en caso de duda, al delegado de protección de datos: “Apple solo usa tus datos personales cuando existe un fundamento jurídico válido para hacerlo. Según las circunstancias, Apple podrá utilizar tu consentimiento o el hecho de que el tratamiento es necesario para satisfacer un contrato contigo, para proteger tus intereses vitales o los de otras personas o para cumplir la ley. También podremos tratar tus datos personales cuando creamos que actuamos en nuestro interés legítimo o en el de otros terceros, tomando en consideración tus intereses, derechos y expectativas. Si tienes alguna pregunta acerca del fundamento jurídico, puedes ponerte en contacto con el delegado de protección de datos en apple.com/es/privacy/contact”.

Sin embargo, a pesar de que consideramos que la base legítima para el consentimiento al tratamiento de datos personales ex art. 6.I, letra a) RGPD es la más adecuada, es importante distinguir entre el consentimiento contractual y el consentimiento para el tratamiento de datos personales, pues no es lo mismo y muchas veces en los clausulados uno y otro consentimiento aparecen ligados¹⁴⁴. En este sentido, el CEPD señala que “Dependiendo de las circunstancias, los interesados pueden creer erróneamente que prestan su consentimiento en consonancia con lo dispuesto en el artículo 6, apartado I, letra a), al firmar el contrato o aceptar las condiciones del servicio. Al mismo tiempo, el responsable del tratamiento puede asumir erróneamente que la firma del contrato equivale a un consentimiento en el sentido del artículo 6, apartado I, letra a). Sin embargo, se trata de conceptos totalmente diferentes¹⁴⁵. Es importante distinguir entre aceptar las condiciones del servicio al celebrar un contrato y prestar el consentimiento en el sentido del artículo 6, apartado I, letra a), puesto que estos conceptos se encuentran sujetos a requisitos distintos y tienen consecuencias jurídicas diferentes¹⁴⁶. Así lo ratifica también el GT29 que indica 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 personales¹⁴⁷. De ahí que pueda afirmarse que muchos modelos de negocio que proliferan actualmente en internet no respetan algunas de estas exigencias establecidas por la normativa de protección de consumidores, aunque, curiosamente, es cierto que tampoco tiene ninguna consecuencia sancionatoria.

144 Estos dos consentimientos, a pesar de ser distintos, coinciden en que son contratos de adhesión, es decir, el consumidor se adhiere a una serie de cláusulas no negociadas individualmente cuya validez dependerá del cumplimiento de los oportunos requisitos legales. De esta forma, deberá superar los filtros de incorporación, transparencia, abusividad y legalidad.

145 Vid., en este sentido, CÁMARA LAPUENTE, S.: “Nuevos perfiles del consentimiento en la contratación digital en la Unión Europea: ¿navegar es contratar (servicios digitales ‘gratuitos’)?”, en AA.VV.: *Estudios de Derecho Contractual Europeo: nuevos problemas, nuevas reglas* (dir. por F. GÓMEZ POMAR e I. FERNÁNDEZ CHACÓN), Aranzadi-Thomson Reuters, Cizur Menor (Navarra), 2022, p. 340, quien afirma que el usuario debe emitir un consentimiento doble y diferenciado que no siempre la estructura del portal empresarial ayudará a distinguir: por una parte el consentimiento “reforzado”, específico y que “se distinga claramente de los demás asuntos” para el tratamiento de los datos personales del usuario o interesado (arts. 7.2 y 4.11 RGPD) y, por otra parte, el consentimiento genuinamente contractual que genera el vínculo obligacional.

146 En el mismo sentido, el SEPD ya advertía de la necesidad de evitar esta confusión en el referido Dictamen sobre la propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales (Opinion 8/2018 on the legislative package “A New Deal for Consumers”, consultar en: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-legislative-package-new-deal-consumers_en), donde señala que el concepto de contratos de suministro de contenidos o servicios digitales por el que los consumidores facilitan sus datos personales, en lugar de pagar con dinero, podría inducir a error a los proveedores de servicios, a quienes se haría creer que el tratamiento de datos basado en el consentimiento en el contexto de un contrato es legalmente conforme en todos los casos, incluso cuando no se cumplen las condiciones para un consentimiento válido establecidas en el RGPD, lo cual socavaría la seguridad jurídica.

147 *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, de 4 de mayo de 2020, p. 18. (Consultar en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf).

En cualquier caso, como ya nos hemos referido anteriormente, las condiciones para el tratamiento lícito de los datos personales no se deben regular ni por la DCSD ni por el TRLGDCU, dado que se trata de una cuestión ya regulada por el RGPD¹⁴⁸; y, por tanto, para valorar la licitud del tratamiento de los datos relacionados con un contrato de suministro de contenidos o servicios digitales tendremos que estar a las disposiciones del RGPD. Ahora bien, tanto la DCSD como el TRLGDCU deben complementarse con el RGPD, pero, en caso de conflicto, prevalecerá este último¹⁴⁹. Sin embargo, ello no está exento de problemas jurídicos que se exponen en el siguiente apartado.

IX. PROBLEMAS JURÍDICOS QUE SE PLANTEAN EN RELACIÓN CON EL RGPD.

Es cierto que la DCSD y el TRLGDCU deben complementarse con el RGPD, pero en la interacción entre la normativa de consumo y la normativa de protección de datos surgen algunos problemas que merecen ser tratados¹⁵⁰.

I. La contradicción entre la obligación de ceder los datos personales como contraprestación y el derecho a revocar el consentimiento.

Conviene poner de manifiesto que, carácter general, el tratamiento de datos personales en relación con un contrato de suministro de contenidos o servicios digitales será lícito si se ajusta a lo establecido por el RGPD. Sin embargo, existe una clara contradicción entre la obligación de ceder los datos personales y la aceptación de su tratamiento, con el principio de libre revocación del consentimiento establecido en el art. 7.3 RGPD.

Este ha sido uno de los problemas más debatidos por la doctrina¹⁵¹, especialmente en lo que se refiere a las consecuencias posteriores al contrato.

148 Cdo. 38 DCSD.

149 Art. 114.1, párrafo 2º TRLGDCU y art. 3.8, párrafo 2º DCSD y Cdo. 37 DCSD.

150 Se trata de una compleja interacción entre la normativa de protección de datos personales y de derecho del consumo que llevó a la 41ª Conferencia Internacional de Autoridades de Protección de Datos (octubre, 2019) a poner de manifiesto la necesidad de aumentar la cooperación entre las autoridades de protección de datos, de consumo y de defensa de la competencia, con el fin de lograr unos altos niveles de protección de datos claros y transparentes en la economía digital. *Vid.*, en este sentido, *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* (Consultar en: https://edps.europa.eu/sites/default/files/publication/dccwg-resolution_adopted_en.pdf). En esta línea, MILA RAFAEL, R.: "Datos personales", cit., p. 411, afirma que la Directiva presentaba el gran reto de dar respuesta a las cuestiones derivadas de la interacción de las reglas de derecho contractual con las normas que regulan el tratamiento de los datos personales previstas en el RGPD.

151 *Vid.* entre otros, CÁMARA LAPUENTE, S.: "Un primer balance", cit., pp. 23-24; MARTÍNEZ VELENCOSO, L.M. y SANCHO LÓPEZ, M.: "El nuevo concepto de onerosidad", cit., pp. 11-13; DE BARRÓN ARNICHERS, P.: "La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)", *Cuadernos europeos de Deusto*, núm. 61, 2019, pp. 60-62; METZGER, A.: "Un modelo de mercado", cit., p. 129; o STAUDENMAYER, D.: "Comentario al art. 3 Directiva (UE) 2019/770", cit., p. 73.

Sin embargo, la revocación del consentimiento no debe afectar a la validez del contrato¹⁵². En cualquier caso, el legislador español, consciente de la situación, ha previsto la solución para el caso de que el consumidor decida retirar su consentimiento. En este sentido, el art. 119 ter. 7 TRLGDCU permite al empresario, en el referido caso, resolver el contrato siempre y cuando el suministro de los contenidos o servicios digitales sea continuo o consista en una serie de actos individuales y se encuentre pendiente de ejecutar en todo o en parte¹⁵³. Además, el ejercicio de estos derechos por parte del consumidor no supondrá, en ningún caso, el pago de penalización alguna a su cargo. De esta forma, la revocación del consentimiento para el tratamiento de datos personales no implica la revocación del consentimiento contractual, pero sí que se faculta al empresario para resolver el contrato

Ahora bien, este carácter revocable del consentimiento implica dejar sin efecto la amplia excepción al desistimiento en los contratos de suministro de contenidos y servicios digitales prevista en el art. 103, letras a) y m) TRLGDCU, dado que el consumidor titular de los datos siempre podría desvincularse del contrato revocando su consentimiento al tratamiento¹⁵⁴, 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 dineraria¹⁵⁵.

Por su parte, se ha advertido¹⁵⁶ que la revocación del consentimiento choca claramente con el artículo 1.256 CC, según el cual la validez y cumplimiento de los contratos no puede dejarse al arbitrio de una de las partes, en la medida en que, en este tipo de contratos, el cumplimiento de una parte del contrato queda al arbitrio de uno de los contratantes (el titular de los datos).

152 METZGER, A.: "Un modelo de mercado", cit., p. 129.

153 No obstante, esta solución, en algunos casos, puede no ser la más adecuada, dado que, como advierte STAUDENMAYER, D.: "Comentario al art. 3 Directiva (UE) 2019/770", cit., p. 73, en la práctica, los datos personales cedidos como contraprestación se monetizan muy rápidamente.

154 Es por ello que autores como DE FRANCESCHI, A.: "Personal Data as Counter", cit., p. 69, afirman que sería razonable excluir la aplicabilidad de la excepción al derecho de desistimiento en el caso de contratos en que los datos personales constituyan la contraprestación, aunque el citado autor advierte que esta (deseable) inaplicabilidad podría generar una disparidad de tratamiento entre "pagar con dinero" y "pagar con datos".

155 GARCÍA PÉREZ, R.M.: "Interacción entre protección", cit., p. 190. En el mismo sentido, CARRASCO PERERA, Á.: "Resolución de contrato pagado con datos personales como precio", *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2022, p. 2; GARCÍA-RIPOLL MONTIJANO, M.: "La resolución por el consumidor del contrato de suministro de contenidos y servicios digitales", en AA.VV.: *Contratación en el entorno digital* (coord. por I. GONZÁLEZ PACANOWSKA y M.C. PLANA ARNALDOS), Aranzadi, Cizur Menor (Navarra), 2023, p. 266; o FERNÁNDEZ CHACÓN, I.: "Caracterización y régimen aplicable", cit., pp. 251-252.

156 GARCÍA PÉREZ, R.M.: "Interacción entre protección", cit., p. 191. *Vid.*, en un sentido similar, CERVILLA GARZÓN, M.D.: "Obligaciones y remedios de las partes en los contratos de servicios relacionados", en AA.VV.: *El derecho común europeo de la compraventa y la modernización del derecho de contratos* (ed. por A. VAQUER ALOY, et.al.), Atelier, Barcelona, 2015, p. 667, y CONESA CABALLERO, O.: "El encaje contractual", cit., p. 159. Si bien este último autor matiza que existe una diferencia sustancial con respecto a los derechos al honor, intimidad personal y propia imagen, pues la ley en estos últimos derechos regula un consentimiento, cuya revocación puede llevarse a cabo en cualquier momento, pero que, no obstante, es susceptible de generar una indemnización por los daños y perjuicios causados.

2. La incidencia en el contrato de un consentimiento inválido al tratamiento de datos personales.

Uno de los problemas más complejos que se presenta en la interacción entre la normativa de consumo y de protección de datos versa sobre cómo incide en el contrato de suministro de contenidos y servicios digitales el consentimiento del consumidor que no se considera válido por no reunir los requisitos del art. 6.1, letra a) RGPD. Al respecto, cabe señalar que si la ilicitud del consentimiento incidiera en la eficacia del contrato celebrado, provocando su invalidez, esto conduciría a la inaplicación de los remedios protectores previstos para el consumidor en el TRLGDCU, quedando asimismo el empresario liberado de todas las responsabilidades derivadas del referido texto normativo. De esta forma, el incumplimiento por el responsable del tratamiento de las exigencias derivadas del RGPD beneficiaría a quien provoca tal incumplimiento¹⁵⁷. En otras palabras, si el proveedor no obtuviese el consentimiento conforme a la normativa de protección de datos, el contrato sería ineficaz y, por ende, se beneficiaría de la no aplicación de las responsabilidades previstas en el TRLGDCU, privando al consumidor de los remedios contractuales, lo que carecería de toda lógica y coherencia.

Por ello, en orden a superar este problema planteado, cabe separar el consentimiento contractual y el consentimiento conforme al RGPD, de manera que la ilicitud de este último consentimiento no debe afectar al consentimiento contractual y, en consecuencia, no afectar a la validez del contrato celebrado¹⁵⁸. De esta forma, un consentimiento para el tratamiento de datos personales no conforme con el RGPD no provoca, por sí solo, la invalidez del contrato de

157 Vid., en la misma línea, HACKER, P.: "Regulating the Economic Impact", cit., p. 59; y METZGER, A.: "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSE, R. SCHULZE y D. STAUDEMANYER), Nomos/Hart, Baden-Baden (Munich), 2020, p. 34.

158 Aprovechando esta distinción entre consentimiento para el tratamiento de datos personales y consentimiento contractual, compartimos la opinión de CÁMARA LAPUENTE, S.: "Nuevos perfiles del consentimiento", cit., pp. 383-385, quien propone trasvasar los rasgos y requisitos del consentimiento para el tratamiento de datos personales establecidos en el RGPD al consentimiento para celebrar el contrato electrónico y aceptar sus condiciones generales. En este sentido, se echa en falta una regla general que exija que el consentimiento al objeto del contrato sea libre, inequívoco, informado, específico y con una clara acción afirmativa, pues ello supondría un avance para la seguridad jurídica y para la protección de los usuarios digitales, con un estándar europeo que no dependiese de los regímenes nacionales de forma tan incierta. También defienden esta distinción entre consentimiento contractual y consentimiento al tratamiento de datos TRIPODI, E.M.: "Consumi digitali e dati personali", cit., pp. 283-284; e IRTI, C.: *Consenso "negoziato" e circolazione dei dati personali*, Giappichelli, Torino, 2021, pp. 74-79. Esta última autora matiza que, dado que se trata de dos consentimientos distintos, el consentimiento al tratamiento de los datos no debe ser un elemento del contrato, sino que debe ser ajeno al mismo, teniendo naturaleza autorizativa (no obligatoria, debiendo ser libre) y carácter unilateral. Por su parte, para conceptualizar esta cuestión METZGER, A.: "A Market Model", cit., p. 34, trae a colación el "principio de abstracción", que es uno de los principios básicos del Derecho civil alemán, en virtud del cual hay que separar el acuerdo sobre los derechos y obligaciones de las partes y las transacciones reales. Así, uno puede ser válido, mientras que el otro puede ser nulo. Es cierto que el autor matiza que el consentimiento para el tratamiento de datos personales no es una transacción *in rem stricto sensu*, pero que, no obstante, todavía tiene sentido distinguir entre la promesa contractual de proporcionar datos y dar el consentimiento y el cumplimiento de esta promesa.

suministro de contenidos o servicios digitales¹⁵⁹. Todo ello, sin perjuicio del derecho del consumidor a pedir la indemnización por daños y perjuicios reconocido en el art. 8.1, letra c) TRLGDCU.

3. Sobre las limitaciones previstas en los arts. 7.4 RGPD y 6.3 LOPDGD.

Cuando el tratamiento de datos personales cedidos como contraprestación a cambio del suministro de contenidos y servicios digitales se basa en el consentimiento ex art. 6.1, letra a) RGPD, las disposiciones previstas en el RGPD deben ponerse en relación con aquellas previstas en la LOPDGD, pues el RGPD reconoce “un margen de maniobra para que los Estados miembros especifiquen sus normas” y, en consecuencia, “no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito”¹⁶⁰. De esta forma, además de los requisitos necesarios que debe reunir la manifestación de voluntad previstos en el art. 4.11 RGPD¹⁶¹, en el art. 7 RGPD se prevén las condiciones para que el consentimiento al tratamiento de datos sea válido, entre las que, en lo que aquí resulta de interés, destaca la prevista en el art. 7.4 RGPD, la cual hay que poner en relación con aquella prevista en el art. 6.3 LOPDGD.

Así, por un lado, el art. 7.4 RGPD establece que “Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato”. Mientras que, por otro lado, el art. 6.3 LOPDGD indica que “No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual”.

Como se puede apreciar, el art. 6.3 LOPDGD establece un límite mucho más restrictivo que el previsto por el art. 7.4 RGPD, pues mientras el art. 7.4 RGPD se limita simplemente a tener en cuenta “en la mayor medida posible” si la ejecución del contrato se supedita al consentimiento para el tratamiento de datos personales, el art. 6.3 LOPDGD establece un mandato directo al suministrador mediante el cual se le niega la posibilidad de que la ejecución del contrato se

159 Vid. en este sentido GARCÍA PÉREZ, R.M.: “Interacción entre protección”, cit., pp. 191-192; y METZGER, A.: “Un modelo de mercado”, cit., p.128 quien afirma que un consentimiento inválido puede ser suficiente para aplicar la DCSD si se cumplen los otros requisitos. A este respecto, reviste cierta importancia distinguir entre las obligaciones contractuales válidas o no válidas entre el empresario y el consumidor, por una parte, y el consentimiento válido o inválido del interesado en el tratamiento de los datos por otra.

160 Cdo. 10 RGPD.

161 Vid., *supra* apartado 5.

supedite al consentimiento para el tratamiento de datos personales que no guarden una relación con el mantenimiento, desarrollo o control de la relación contractual. De esta forma, conforme al art. 7.4 RGPD cabe la posibilidad de que, a pesar de que la ejecución del contrato se supedite al consentimiento para el tratamiento de los datos personales, dicho consentimiento pueda ser válido según las circunstancias. En cambio, según el art. 6.3 LOPDDGPP, cuando ello ocurra, parece ser que el consentimiento –de forma automática- no se considerará válido.

Ahora bien, el contenido del art. 7.4 RGPD puesto en relación con el art. 6.3 LOPDDGPP, puede dar lugar a interpretaciones en un doble sentido:

Por un lado, la primera interpretación que cabe considerar es que el cumplimiento de los contratos no puede hacerse depender de que el consumidor o usuario consienta el tratamiento de sus datos personales para finalidades distintas de las establecidas en los arts. 7.4 RGPD y 6.3 LOPDDGPP, esto es, que no sean necesarios para la ejecución del contrato¹⁶² o para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual. En este sentido, se prohibiría hacer depender la ejecución del contrato de la prestación del consentimiento sobre el tratamiento de los datos personales cuando éstos se requirieran para otras finalidades más allá de cuestiones técnicas¹⁶³. De esta forma, solamente cabría supeditar la ejecución del contrato al consentimiento para el tratamiento de los datos personales cuando dicho tratamiento fuese estrictamente necesario para que el empresario pudiera suministrar el contenido o servicio digital, pero, como ya sabemos, la realidad es otra muy distinta: las empresas que suministran contenidos y servicios digitales no recaban los datos únicamente por cuestiones técnicas o legales, sino que los utilizan para otras finalidades, especialmente para fines comerciales. Por tanto, si partimos de este presupuesto, aquí se proponen tres posibles soluciones:

a) La primera solución es que el consumidor o usuario pueda negarse a prestar su consentimiento para el tratamiento de sus datos personales y, aun así, pueda acceder a los contenidos o servicios digitales, ya que el proveedor no puede condicionar el acceso a los mismos a que el consumidor dé su consentimiento¹⁶⁴, pues, si partimos de una interpretación estricta según la cual la ejecución del contrato no puede hacerse depender del consentimiento del usuario, el empresario no puede obligar al consumidor a consentir el tratamiento de sus datos personales a cambio del contenido o servicio digital. Si lo hiciera, este consentimiento no sería emitido libremente y, en consecuencia, sería ilícito. No obstante, partiendo del

162 Sobre la “necesariedad” de los datos personales para la ejecución del contrato, *vid.*, *supra* apartado 8.1.

163 En tal caso, cabe advertir que la base jurídica que legitimaría el tratamiento de datos personales no sería el consentimiento *ex art.* 6.1, letra a) RGPD, sino la base contractual establecida en el art. 6.1, letra b) RGPD.

164 *Vid.*, en esta misma línea, SÁNCHEZ LERÍA, R.: “Los datos personales como contraprestación en la legislación de consumo”, *Actualidad Civil*, núm. 3, 2022, p. 7.

supuesto de que el consumidor se niega a prestar el consentimiento y, a pesar de ello, puede acceder a los contenidos o servicios digitales, lo que sí que existe es una renuncia a los derechos reconocidos en la propia DCSD y en el TRLGCDU, pues el ámbito de aplicación de ambos textos normativos recae sobre aquellos contratos en los que el consumidor “facilita o se comprometa a facilitar datos personales al empresario (...)”¹⁶⁵. De esta forma, el consumidor o usuario podría acceder a los contenidos y servicios digitales, pero, en caso de falta de conformidad o incumplimiento del empresario, aquel no podría recurrir a las medidas correctoras que se prevén en los referidos textos normativos. No obstante, se trata de una solución poco convincente, pues, si bien es cierto que el empresario no debería responder por los incumplimientos o faltas de conformidad, no es menos cierto que tampoco recibiría contraprestación alguna por la prestación del contenido o servicio digital¹⁶⁶. Por tanto, imponerle la obligación de suministrar un contenido o servicio digital a cambio de nada tampoco sería viable.

b) La segunda solución es considerar que la decisión sobre si la contraprestación por el contenido o servicio digital consiste en la cesión de uso de datos personales o en el pago de un precio en dinero recaiga en el consumidor o usuario¹⁶⁷. Es decir, se le debería dar al consumidor o usuario la posibilidad de que eligiese entre las dos modalidades de contraprestación: o bien dar su consentimiento para el tratamiento de datos personales, o bien pagar una cantidad en dinero equivalente al valor de los datos personales. De esta forma, se le ofrecerían al consumidor dos alternativas de pago, de manera que evitaríamos que el consumidor se viese obligado a consentir en el tratamiento de sus datos personales como única vía para disfrutar de los contenidos o servicios digitales. En consecuencia, podría decirse que el suministro de contenidos o servicios digitales no quedaría supeditado únicamente al consentimiento para el tratamiento de datos personales y, por ende, si el consumidor decidiera prestar su consentimiento al tratamiento de datos personales, éste podría considerarse como libremente prestado.

c) Por último, la tercera solución podría consistir en que el suministrador de contenidos y servicios digitales incluyese en las condiciones generales una cláusula conforme a la cual el usuario se comprometiera a aceptar todas las cookies

165 Vid., en este sentido, los arts. 3.1 DCSD y 59.4 TRLGDCU.

166 A este respecto, MARTÍNEZ CALVO, J. “Dualidad normativa en la regulación”, cit., p. 1175, señala que esto sería tanto como hacer recaer en el consumidor la decisión sobre la gratuidad u onerosidad del contrato, de manera que, si el consumidor se negara a prestar su consentimiento, el contrato que, en un principio, era oneroso, se convertiría en gratuito, dado que el consumidor no llevaría a cabo contraprestación ninguna, lo que, además, contravendría lo dispuesto por el art. 1.256 CC, el cual señala que “la validez y el cumplimiento de los contratos no pueden dejarse al arbitrio de uno de los contratantes”. Opina de igual manera CONESA CABALLERO, Ó.: “El encaje contractual”, cit., pp. 156-157.

167 De hecho, esta falta de posibilidades alternativas de que carece el consumidor o usuario es calificada por METZGER, A.: “Un modelo de mercado”, cit., p.137, como una “causa de insuficiencia de mercado”, pues, como señala el autor, en un mercado que funcione bien, los consumidores deben poder elegir entre diferentes servicios y ofertas. Por tanto, deberían tener la posibilidad de elegir entre servicios de pago y servicios basados en el tratamiento de datos personales.

propuestas por el suministrador en el contrato¹⁶⁸, de forma que cabría entender que el tratamiento de los datos personales tuviera por finalidad “el mantenimiento, desarrollo o control de la relación contractual”. Esta interpretación sería *hecha a medida* para las empresas suministradoras de contenidos y servicios digitales, dada la predisposición del contenido del contrato por parte de estas empresas¹⁶⁹. Sin embargo, no creemos que esta solución fuese correcta, dado que el compromiso a aceptar todas las *cookies* a través de una cláusula contravendría el art. 6.1, letra a) RGPD, en virtud del cual el consumidor debe prestar su consentimiento por separado para cada uno de los fines específicos a los que se van a destinar sus datos.

Por otro lado, la segunda de las interpretaciones que cabe extraer de acuerdo al art. 7.4 RGPD, puesto en relación con lo dispuesto por el art. 6.3 LOPDGDD, es una interpretación restrictiva que se fundamenta principalmente en la protección de la libertad –autodeterminación– del usuario, quien, además, en los contratos de suministro de contenidos y servicios digitales ve coartada por completo su libertad contractual –autonormación– debido a la predisposición unilateral del contrato por el suministrador del contenido o servicio digital¹⁷⁰. Por tanto, lo que cabe extraer de una interpretación restrictiva de estos artículos es que los mismos encuentran su fundamento en garantizar que el interesado pueda prestar su consentimiento de forma totalmente libre y que, en consecuencia, se adopten todas las garantías necesarias para que el consentimiento sea válido¹⁷¹. En este sentido, si el consumidor es consciente de la finalidad para la que van a ser destinados sus datos, y éste acepta de forma totalmente libre el tratamiento de los mismos y con todas las garantías y requisitos para velar por la validez del consentimiento, no creemos que exista inconveniente en que el tratamiento de los datos personales pueda convertirse en prestación contractual y, por ende, que le afecten las limitaciones que se expresan en los arts. 7.4 RGPD y 6.3 LOPDGDD, pues, como muy acertadamente señala parte de la doctrina¹⁷² de lo que se trata es de que el individuo tome sus propias decisiones y asuma la responsabilidad

168 Sobre las obligaciones que debe cumplir el prestador del servicio respecto a las *cookies*, *vid.*, SANTOS MORÓN, M.J.: “Consumidor y nuevas tecnologías”, *cit.*, pp. 310-311.

169 DOMÍNGUEZ YAMASAKI, M. I.: “El tratamiento de datos personales”, *cit.*, p. 110.

170 *Ibidem*, p. 112.

171 Aquí puede resultar interesante traer a colación la distinción entre el consentimiento al tratamiento de datos y el consentimiento contractual, pues como señala METZGER, A.: “Un modelo de mercado”, *cit.*, pp.128-129, esta distinción es también pertinente para salvar la prohibición de vincular el contrato y el consentimiento del art. 7.4 RGPD, ya que, *a priori*, puede parecer que exista una prohibición explícita de cualquier ligazón entre consentimiento y ejecución del contrato, pero la prestación de autorización al tratamiento en el mero marco de un contrato no debe considerarse como un indicio de coacción ni de toma de decisiones defectuosas. Además, señala el autor que, incluso si el consentimiento fuera inválido en un caso determinado en virtud del art. 7.4 RGPD, ello no daría lugar automáticamente a la inaplicabilidad de la DCSD.

172 NAVAS NAVARRO, S.: “El valor de los datos personales”, *cit.*, p. 120.

derivada de las mismas¹⁷³. La acción paternalista debería crear las condiciones necesarias, mediante la información transparente, para que el individuo pudiera tomar su decisión cabalmente y con conocimiento de causa¹⁷⁴. En definitiva, se trata de empoderar al individuo; no de sobreprotegerlo.

Sin embargo, el problema que se plantea es que las “políticas de datos” y “declaraciones de privacidad” son demasiado largas y complejas y, en consecuencia, los interesados o titulares de los datos no las llegan a leer completamente pues les resulta algo demasiado extenso y farragoso¹⁷⁵, más aún cuando se trata de legos en la materia¹⁷⁶, aunque, incluso en el caso de que las partes se encontraran en una posición de simetría contractual, las limitaciones cognitivas y racionales de los interesados no les permitiría evaluar de forma efectiva el contenido y los efectos del consentimiento prestado respecto a la política de privacidad¹⁷⁷ y, en consecuencia, no ser conscientes de que pueden estar poniendo en juego su “privacidad”¹⁷⁸.

No obstante, no creemos que la culpa de que las “políticas de datos” y “declaraciones de privacidad” sean largas y complejas de entender deba recaer solamente en los suministradores de contenidos y servicios digitales, sino que, en su mayor parte, se debe a las regulaciones europeas y nacionales en materia de protección de datos. Los suministradores de contenidos y servicios digitales simplemente lo que hacen es establecer en sus páginas web “políticas de datos” y “declaraciones de privacidad” adecuadas a la normativa vigente. De ahí que, desde nuestro punto de vista, una de las soluciones para acabar con este problema consistiría en elaborar unos modelos de información claros y sencillos que se adecuasen a las capacidades del consumidor medio, evitando los textos largos

173 En este sentido, GARCÍA HERNÁNDEZ, A.: “Cuando los usuarios se convierten en el producto: Google Maps se suma a la tendencia ‘Datos a cambio de uso gratuito’”, *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2021, p. 6, afirma que, en el caso de las plataformas digitales, concretamente en el supuesto de *Google Maps*, si el proveedor limita los servicios prestados a los usuarios que no acepten las nuevas condiciones de uso estaría actuando de acuerdo con la legalidad vigente.

174 En un sentido similar apunta METZGER, A.: “Un modelo de mercado”, cit., p.130

175 En esta línea, se pronuncia DE BARRÓN ARNICHES, P.: “La pérdida de privacidad”, cit., p. 54, quien afirma que existe una tendencia por parte de los consumidores a aceptar fácilmente estos contratos estándar, independientemente de si realmente entienden las consecuencias, o simplemente, porque no tienen otra alternativa real si quieren acceder a estos servicios digitales.

176 *Vid.*, en el mismo sentido, BEN SHAHAR, O. y STRAHILEVITZ, L.J.: “Contracting over Privacy: Introduction”, *Journal of Legal Studies*, vol. 45, 2016, p. 1-13 (consultar en: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2455&context=law_and_economics); ARTIGOT GOLOBARDES, M.: “La contratación digital”, cit., p. 473; y REIDENBERG, J., et.al.: “Ambiguity in Privacy Policies and the Impact of Regulation”, *Journal of Legal Studies*, vol. 45, 2016, pp. 1-29 (consultar en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715164).

177 ARTIGOT GOLOBARDES, M.: “La contratación digital”, cit., p. 471.

178 SANTOS MORÓN, M.J.: “Consumidor y nuevas tecnologías”, cit., p. 304.

y en letra pequeña¹⁷⁹. Una posibilidad serían los “iconos de privacidad”¹⁸⁰ como forma de mejorar la autodeterminación del consumidor en este tipo de contratos y ayudarle a tomar decisiones con conocimiento de causa¹⁸¹. Sin embargo, como advierte una parte de la doctrina¹⁸², a pesar de que los consumidores estén bien informados, éstos pueden tomar decisiones que van en contra de sus preferencias a largo plazo, pues una cosa es reconocer la importancia de una gestión prudente de los propios datos personales y otra es vivir de acuerdo con este principio si el consumidor se siente tentado por ofertas de contenidos y servicios digitales que se basan en la recopilación de sus datos.

Ahora bien, para evitar que los consumidores puedan cambiar de opinión respecto al tratamiento de sus datos en un medio o largo plazo y, en consecuencia, hacer valer en cualquier momento los derechos que les reconoce la normativa de protección de datos, una solución que se ha propuesto es la creación de plataformas que permitan a los usuarios gestionar de forma sencilla y segura permisos para el tratamiento de sus datos personales en diferentes contextos y para diferentes finalidades¹⁸³. Es lo que se conoce como “servicios de datos personales” (en inglés “personal data services” o “PDS”), aunque para que ello funcionase adecuadamente sería necesario implantar fuertes medidas de seguridad, ya que una misma plataforma sería la encargada de almacenar una gran cantidad de datos personales.

179 Pues, como señalan COFONE, I. y ROBERTSON, A.: “Consumer Privacy in a Behavioral World”, *Hastings Law Journal*, vol. 69, núm. 6, 2018, pp. 1471-1507 (consultar en: https://repository.uchastings.edu/hastings_law_journal/vol69/iss6/11/), uno de los problemas es que la gran cantidad de información que se proporciona a los interesados hace que no puedan distinguir entre aquello que es relevante o no y entre lo que es deseable o aceptable de acuerdo con sus preferencias.

180 Los “iconos de privacidad” son representaciones gráficas utilizadas en línea para proporcionar información rápida y visual sobre cómo se manejan los datos personales y la privacidad en un sitio web o una aplicación. Sobre esta propuesta de los iconos de privacidad, *vid.*, en un sentido similar, EFRONI, Z., et. al.: “Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing”, *European Data Protection Law Review (EDPL)*, núm. 3, 2019, pp. 352 y ss.

181 De hecho, ya existen iniciativas como *Consent Commons* (<https://consentcommons.com/>) que han creado un sistema de iconos que resume de un vistazo la información legal que recoge el consentimiento cuando se recaban datos de personas físicas en entornos online y apps, y que nace con el objetivo de facilitar la comprensión y la transparencia de los documentos legales para las personas. En este sentido, bajo un icono central o iconos centrales, que representan para qué van a usarse los datos (lo que el RGPD llama la “finalidad”), se construye el resto de los elementos que el RGPD exige: si se va a ceder a terceros y para qué, si se van a almacenar en la UE o fuera, si se recogen en el formulario, en un contrato, etc.

182 METZGER, A.: “Un modelo de mercado”, *cit.*, p. 138.

183 Sin embargo, como advierte GIL GONZÁLEZ, “Big Data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?”, *Diario La Ley*, núm. 9050, 2017, p. 12, este modelo únicamente puede tener sentido en un escenario en el que los derechos de portabilidad de los datos sean efectivos, de modo que los individuos puedan trasladar sus datos de un proveedor a otro. En tal sentido, este modelo sería relevante en aquellos medios que permitiesen asegurar la autenticación de la identidad de los sujetos que debieran gestionar su identidad digital y sus datos personales.

BIBLIOGRAFÍA

ABA CATORIA, A.: "Principios de protección de datos", en AA.VV.: *Comentarios a la Nueva Ley de Protección de Datos* (coord. por A. TURNES VILLANUEVA), Dilex, Madrid, 2020, pp. 25-47.

ALIÑO SEHWERT, J.J.: "La protección del consumidor digital: los datos personales en el comercio electrónico", *Revista Jurídica sobre Consumidores y Usuarios*, núm. 3, 2018, pp. 97-115.

AMÉRIGO ALONSO, J.: "Objeto y ámbito de aplicación", en AA.VV.: *Tratado de protección de datos* (dir. por A. RALLO LOMBARTE), Tirant lo Blanch, Valencia, 2019, pp. 79-104.

AMMERMAN YEBRA, J.: "El alcance de las cláusulas contenidas en los contratos de suministro de contenidos y servicios digitales que prevén la interacción del usuario con el servicio mediante comandos de voz", *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, pp. 1110-1023.

APARICIO VAQUERO, J.P.: "Principios del tratamiento y derechos de los interesados en la nueva normativa de protección de datos personales", *Rued@: Universidad Ética y Derechos*, núm. 3-4, 2019, pp. 19-40.

ARROYO VENDRELL, T. y SCHULZE, R.: "Contratos de contenidos digitales: Introducción", en AA.VV.: *Verträge über digitale Inhalte und digitale Dienstleistungen* (coord. por J. KINDL, T. ARROYO VENDRELL y B. GSELL), Nomos Verlagsgesellschaft, Baden-Baden (Alemania), 2018, pp. 11-20.

ARTIGOT GOLOBARDES, M.: "La contratación digital con consumidores en dos actos: las políticas de privacidad en la antesala de la contratación digital", en AA.VV.: *Estudios de Derecho Contractual Europeo: nuevos problemas, nuevas reglas* (dir. por F. GÓMEZ POMAR e I. FERNÁNDEZ CHACÓN), Aranzadi-Thomson Reuters, Cizur Menor (Navarra), 2022, pp. 451-493.

BEN SHAHAR, O. y STRAHILEVITZ, L.J.: "Contracting over Privacy: Introduction", *Journal of Legal Studies*, vol. 45, 2016, pp. 1-11.

CABALLERO TRENADO, L.: "Cookies y consentimiento", *Revista Crítica de Derecho Inmobiliario*, núm. 96, 2020, pp. 3227-3239.

CÁMARA LAPUENTE, S.: "Nuevos perfiles del consentimiento en la contratación digital en la Unión Europea: ¿navegar es contratar (servicios digitales 'gratuitos')?", en AA.VV.: *Estudios de Derecho Contractual Europeo: nuevos problemas, nuevas reglas*

(dir. por F. GÓMEZ POMAR E I. FERNÁNDEZ CHACÓN), Aranzadi-Thomson Reuters, Cizur Menor (Navarra), 2022, pp. 331-405.

- “Un primer balance de las novedades del RDL 7/2021, de 27 de abril, para la defensa de los consumidores en el suministro de contenidos y servicios digitales”, *Diario La Ley*, núm. 9887, 2021, pp. 1-38.
- “Resolución contractual y destino de los datos y contenidos generados por los usuarios de servicios digitales”, *Cuadernos de Derecho Transnacional*, vol. 12, núm. 1, 2020, pp. 838-862.
- “Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad”, en AA.VV.: *El mercado digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, Madrid, 2019, pp. 157-249.
- “Una prospectiva crítica sobre el régimen de los contratos de suministro de contenidos digitales”, en AA.VV.: *Derecho digital: retos y cuestiones actuales* (dir. por F. CAPILLA RONCERO, et.al.), Thomson Reuters - Aranzadi, Cizur Menor (Navarra), 2018, pp. 19-55.

CARRASCO PERERA, Á.: “Resolución de contrato pagado con datos personales como precio”, *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2022, pp. 1-2.

CASTILLO PARRILLA, J.A.: “Los datos personales como contraprestación en la reforma del TRLGDCU y las tensiones normativas entre la economía de los datos y la interpretación garantista del RGPD”, *La Ley Mercantil*, núm. 82, 2021, pp. 1-22.

- “Economía digital y datos entendidos como bienes”, en AA.VV.: *El mercado digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, S.A., Madrid, 2019, pp. 283-305.

CERVILLA GARZÓN, M.D.: “Obligaciones y remedios de las partes en los contratos de servicios relacionados”, en AA.VV.: *El derecho común europeo de la compraventa y la modernización del derecho de contratos* (ed. por A. VAQUER ALOY, et.al.), Atelier, Barcelona, 2015, pp. 645-670.

CHOCRÓN GIRALDEZ, A. M.: “El marco jurídico de la Directiva 2020/1828 en relación con la tutela judicial de los intereses colectivos de los consumidores”, *Cuadernos de Derecho Transnacional*, vol. 14, núm. 2, 2022, pp. 275-293.

COFONE, I. y ROBERTSON, A.: “Consumer Privacy in a Behavioral World”, *Hastings Law Journal*, vol. 69, núm. 6, 2018, pp. 1471-1508.

COFONE, I.: "Beyond Data Ownership", *Cardozo Law Review*, vol. 43, núm. 2, 2021, pp. 501-572.

CONDE ORTÍZ, C.: *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, 2005.

CONESA CABALLERO, Ó.: "El encaje contractual de la cesión de datos de carácter personal: A propósito de la directiva 2019/770 sobre contratos de suministro de contenidos y servicios digitales", *InDret: Revista para el Análisis del Derecho*, núm. 2, 2024, pp. 136-171.

DE BARRÓN ARNICHES, P.: "La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)", *Cuadernos europeos de Deusto*, núm. 61, 2019, pp. 29-65.

DE FRANCESCHI, A.: "Personal Data as Counter-Performance", en AA.VV.: *Privacy and Data Protection in Software Services* (coord. por R. SENIGAGLIA, C. IRTI y A. BERNES), Signapur, 2022, pp. 59-71.

DE PAZ, S. y DE ARCOS TEJERIZO, M.: "La reforma del sistema de acciones de representación a la luz de la Directiva (UE) 2020/1828", *Revista Jurídica Pérez-Llorca*, núm. 7, 2022, pp. 18-46.

DE VERDA Y BEAMONTE, J. R.: "El derecho a la propia imagen", en AA.VV.: *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen* (coord. por J.R. DE VERDA Y BEAMONTE), Aranzadi, Cizur Menor (Navarra), 2007, pp. 145-179.

DOMÍNGUEZ YAMASAKI, M. I.: "El tratamiento de datos personales como prestación contractual. Gratuidad de contenidos y servicios digitales a elección del usuario", *Revista de derecho privado*, núm. 4, 2020, pp. 93-120.

EFRONI, Z., et. al.: "Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing", *European Data Protection Law Review (EDPL)*, núm. 3, 2019, pp. 352-366.

FERNÁNDEZ CHACÓN, I.: "Caracterización y régimen aplicable a los contratos de suministro de contenidos y servicios digitales", en AA.VV.: *El nuevo derecho digital: I. Los contratos de suministro de contenidos y servicios digitales* (dir. por F. GÓMEZ POMAR e I. FERNÁNDEZ CHACÓN), Aranzadi, Madrid, 2024, pp. 121-277.

FERNÁNDEZ PÉREZ, N.: "Contrato sobre contenidos o servicios digitales con consumidores a cambio de datos", en AA.VV.: *Contratación mercantil: digitalización*

y protección del cliente-consumidor (dir. por L.M. MIRANDA SERRANO y J. PAGADOR LÓPEZ, J), Marcial Pons, Madrid, 2023, pp. 55-73.

FRAMIÑÁN SANTAS, J.: "Big data, consentimiento para tratar datos personales y Derecho de Defensa de la competencia", *Revista de Derecho Mercantil*, núm. 310, 2018, pp. 1-6.

FRISANI, C. y VALLI, M.: "Consumatori di beni con elementi digitali e di contenuti e servizi digitali e pratiche commerciali sleali", en AA.VV.: *I diritti dei consumatori digitali* (dir. por R. TORINO), Pacini Giuridica, Pisa, 2023, pp. 179-202.

GARCÍA HERNÁNDEZ, A.: "Cuando los usuarios se convierten en el producto: Google Maps se suma a la tendencia 'Datos a cambio de uso gratuito'", *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2021, pp. 1-7.

- "Datos personales como contraprestación: consecuencias", *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2021, pp. 1-15.
- "Los datos como contraprestación o la pérdida encubierta de la privacidad del individuo a cambio de 'servicios gratuitos'", *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2022, pp. 1-15.

GARCÍA HERRERA, V.: "El pago con datos personales. Incoherencias legislativas derivadas de la configuración de los datos como posible 'contraprestación' en el suministro de contenidos y servicios digitales", *Actualidad Civil*, núm. 1, 2020, pp. 1-12.

GARCÍA PÉREZ, R. M.: "Interacción entre protección del consumidor y protección de datos personales en la Directiva (UE) 2019/770: licitud del tratamiento y conformidad de contenidos y servicios digitales", en AA.VV.: *El derecho privado en el nuevo paradigma digital* (dir. por E. ARROYO AMAYUELAS y S. CÁMARA LAPUENTE), Marcial Pons, Madrid, 2020, pp. 175-208.

- "Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales", *Cuadernos de derecho transnacional*, vol. 12, núm. 1, 2020, pp. 875-907.

GARCÍA RUBIO, M. P.: "La huella y el legado de Federico de Castro en la moderna protección civil de los derechos de la personalidad", en AA.VV.: *Glosas sobre Federico de Castro* (dir. por L. DÍEZ PICAZO), Aranzadi, Cizur Menor (Navarra), 2015, pp. 229-277.

GARCÍA VICENTE, J.R.: "Arts. 1.271-1.272 CC", en AA.VV.: (dir. por R. BERCOVITZ RODRÍGUEZ-CANÓ), *Comentarios al Código Civil* (Tomo VII), Tirant lo Blanch, Valencia, 2013, pp. 9136-9140.

GARCÍA-RIPOLL MONTIJANO, M.: “La resolución por el consumidor del contrato de suministro de contenidos y servicios digitales”, en AA.VV.: *Contratación en el entorno digital* (coord. por I. GONZÁLEZ PACANOWSKA y M.C. PLANA ARNALDOS), Aranzadi, Cizur Menor (Navarra), 2023, pp. 221-270.

- “El consentimiento al tratamiento de datos personales”, en AA.VV.: *Protección de Datos Personales* (coord. por I. GONZÁLEZ PACANOWSKA), Tirant lo Blanch, Valencia, 2020, pp. 79-159.

GAROFALO, A.M.: “Cookies and the Pasive Role of the Data Subject”, en AA.VV.: *Privacy and Data Protection in Software Services* (coord. por R. SENIGAGLIA, C. IRTI y A. BERNES), Signapur, 2022, pp. 73-83.

GIL GONZÁLEZ, E.: “Big Data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?”, *Diario La Ley*, núm. 9050, 2017, pp. 1-15.

GONZÁLEZ HERNÁNDEZ, R.: “La protección del consumidor en la contratación digital”, *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, pp. 1236-1253

GUERRERO PICÓ, M. C.: *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Thomson Reuters - Civitas, Madrid, 2006.

HACKER, P.: “Regulating the Economic Impact of Data as Counter – Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSSE, R. SCHULZE y D. STAUDENMAYER), Nomos/Hart, Baden-Baden (Munich), 2020, pp. 47-76.

HERNÁNDEZ MARTÍN, M. Á.: “La privacidad: una mirada desde la economía”, en AA.VV.: *En torno a la privacidad y la protección de datos en la sociedad de la información* (coord. por J.P. APARICIO VAQUERO y A. BATUECAS CALETRÍO), Comares, Granada, 2015, pp. 1-25.

HERRERÍAS CASTRO, L.: “Contratos de suministro de contenidos y servicios digitales: cuando el precio son tus datos personales”, *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, pp. 1010-1037.

HOOFNAGLE, C.J. y WHITTINGTON, J.: “Free: Accounting for the Costs of the Internet’s Most Popular Price”, *UCLA Law Review*, vol. 61, rev. 606, 2014, pp. 606-670.

IRTI, C.: “Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data”, en AA.VV.: *Privacy and Data Protection in Software Services* (coord. por R. SENIGAGLIA, C. IRTI y A. BERNES), Signapur, 2022, pp. 49-57.

- Consenso “negoziato” e circolazione dei dati personali, Giappichelli, Torino, 2021.

JANEČEK, V. y MALGIERI, G.: “Data Extra Commercium”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSSE, R. SCHULZE y D. STAUDENMAYER), Nomos/Hart, Baden-Baden (Munich), 2020, pp. 95-126.

LANGHANKE, C. y SCHMIDT-KESSEL, M., “Consumer Data as Considetarion”, *Journal of European Consumer and Market Law*, vol. 4, núm. 6, 2015, pp. 218-223.

LOHSSE, S., et.al.: “Data as Counter-Performance – Contract Law 2.0? An Introduction”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSSE, R. SCHULZE y D. STAUDENMAYER), Nomos/Hart, Baden-Baden (Munich), 2020, pp. 9-22.

LÓPEZ JIMÉNEZ, J. M.: “La protección de los consumidores y las acciones de representación: una primera aproximación a la Directiva (UE) 2020/1828”, *Diario la Ley*, núm. 9834, 2021, pp. 1-10.

MAK, V.: “The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content - - In-depth análisis”, *Publications Office*, 2016, pp. 1-28.

MARTÍNEZ CALVO, J.: “Dualidad normativa en la regulación de los contratos gratuitos de suministro de contenidos y servicios digitales: la necesaria armonización entre la Directiva (UE) 2019/770 y el Reglamento (UE) 2016/679”, *Actualidad Jurídica Iberoamericana*, núm. 16, 2022, pp. 1168-1185.

- “Los datos personales como posible contraprestación en los contratos de suministro de contenidos y servicios digitales”, *Indret: Revista para el Análisis del Derecho*, núm. 4, 2021, pp. 88-135.

MARTÍNEZ MARTÍNEZ, R.: “¿Consentimiento o contrato?” (Consultar en: en <http://lopdyseguridad.es/consentimiento-o-contrato/>).

MARTÍNEZ VELENCOSO, L. M. y SANCHO LÓPEZ, M.: “El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?”, *InDret: Revista para el Análisis del Derecho*, núm.1, 2018, pp. 1-36.

MARTÍNEZ VILLASECA, M.: “El interés legítimo como base legitimadora del tratamiento de datos de carácter personal”, *Actualidad administrativa*, núm. 12, 2019, pp. 1-4.

MENÉNDEZ, L.: “¿Qué son las «cookies»?”, *Escritura pública*, núm. 82, 2013, pp. 16-18.

METZGER, A.: “A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services”, en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSE, R. SCHULZE y D. STAUDEMANYER) Nomos/Hart, Baden-Baden (Munich), 2020, pp. 23-46.

- “Un modelo de mercado para los datos personales: estado de la cuestión a partir de la nueva Directiva sobre contenidos y servicios digitales”, en AA.VV.: *El derecho privado en el nuevo paradigma digital* (E. ARROYO AMAYUELAS y S. CÁMARA LAPUENTE), Pons, Madrid, 2020, pp. 121-139.

METZGER, A., et.al.: “Data-Related Aspects of the Digital Content Directive”, *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 9, núm. 1, 2018, pp. 90-109.

MILÀ RAFEL, R.: “Datos personales como contraprestación en la Directiva de contenidos y servicios digitales”, en AA.VV.: *Estudios de Derecho Contractual Europeo: nuevos problemas, nuevas reglas* (dir. por F. GÓMEZ POMAR e I. FERNÁNDEZ CHACÓN), Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2022, pp. 407-450.

MORALES BARCELÓ, J.: “El consentimiento del interesado en materia de protección de Datos del Reglamento UE 2016/679”, en AA.VV.: *El mercado Digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, Madrid, 2019, pp. 307-317.

MORENO GARCÍA, L.: “La tutela colectiva de los consumidores en la Unión Europea: a propósito de la Directiva 2020/1828, de 25 de noviembre de 2020”, *Revista de Derecho Mercantil*, núm. 327, 2023, pp. 1-15.

NAVAS NAVARRO, S.: “El valor de los datos personales en el mercado”, en AA.VV.: *Verträge über digitale Inhalte und digitale Dienstleistungen* (coord. por J. KINDL, T. ARROYO VENDRELL y B. GSELL), Nomos Verlagsgesellschaft, Baden-Baden (Munich), 2018, pp. 101-122.

- “Datos personales y mercado”, en AA.VV.: *Inteligencia artificial: tecnología, derecho* (dir. por S. NAVAS NAVARRO), Tirant lo Blanch, Valencia, 2017, pp. 259-277.
- “Cookies y tecnología análoga: publicidad comportamental online y protección de los datos de carácter personal”, en AA.VV.: *Mercado digital*:

principios y reglas jurídicas (dir. por S. NAVAS NAVARRO y S. CAMACHO CLAVIJO), Tirant lo Blanch, Valencia, 2016, pp. 341-364.

- “El internet de las cosas”, en AA.VV.: *Mercado digital: principios y reglas jurídicas* (dir. por S. NAVAS NAVARRO y S. CAMACHO CLAVIJO), Tirant lo Blanch, Valencia, 2016, pp. 14-48.

ONTIVEROS BAEZA, E.: “El big data y su importancia en el mundo digital”, en AA.VV.: *Economía de los datos. Riqueza 4.0* (dir. por E. ONTIVEROS BAEZA), Fundación Telefónica – Ariel, S.A., 2017, pp. 33-48.

PACHECO JIMÉNEZ, M. N. y LEAL CORONADO, M.: “Nueva moneda de cambio: Nuestros datos personales como pago de contenidos digitales”, *Publicaciones jurídicas del Centro de Estudios de Consumo*, 2017, pp. 1-10.

PAREDES PÉREZ, J.I.: “Acciones de representación resarcitorias y protección de los consumidores como titulares de datos en los contratos de suministro de contenidos y servicios digitales: un estudio en clave de foros de competencia judicial internacional”, en AA.VV.: *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (dir. por J.J. CASTELLÓ PASTOR), Aranzadi - Thomson Reuters, Cizur Menor (Navarra), 2021, pp. 469-501.

PLANA ARNALDOS, M.C.: “Los datos personales como contraprestación”, en AA.VV.: *Protección de Datos Personales* (coord. por I. GONZÁLEZ PACANOWSKA), Tirant lo Blanch, Valencia, 2020, pp. 561-618.

PLAZA PENADÉS, J.: “Aspectos básicos de la protección de datos de carácter personal”, en AA.VV.: *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen* (coord. por J.R. DE VERDA Y BEAMONTE), Aranzadi, Cizur Menor (Navarra), 2007, pp. 119-142.

REIDENBERG, J., et.al, “Ambiguity in Privacy Policies and the Impact of Regulation”, *Journal of Legal Studies*, vol. 45, 2016, pp. 1-29.

RICCIUTO, V.: “Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali”, *Rivista di diritto civile*, vol. 66, núm. 3, 2020, pp. 642-662.

ROBERT, R. y SMIT, L.: “The proposal for a directive on digital content: a complex relationship with data protection law”, *ERA Forum*, vol.19, núm. 2, 2018, pp. 159-177.

ROSELLÓ RUBERT, F. M.: "Las cargas del usuario de servicios de música en continuo (streaming) algunas consideraciones desde la perspectiva de la nueva normativa europea", en AA.VV.: *Plataformas digitales: aspectos jurídicos* (dir. por A. MARTÍNEZ NADAL), Aranzadi, 2021, pp. 247-265.

- "La propuesta de Directiva sobre suministro de contenidos digitales y la protección del consumidor de servicios digitales no retribuidos monetariamente", en AA.VV.: *El mercado Digital en la Unión Europea* (dir. por P. CASTAÑOS CASTRO y J.A. CASTILLO PARRILLA), Reus, Madrid, 2019, pp. 269-282.
- "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", *Revista de Derecho Mercantil*, núm. 303, 2017, pp. 163-190.

SALGADO SEGUÍN, V.: "Intimidad, privacidad y honor en internet", *Telos: cuadernos de comunicación e innovación*, núm. 85, 2010, pp. 69-79.

SÁNCHEZ LERÍA, R.: "Los datos personales como contraprestación en la legislación de consumo", *Actualidad Civil*, núm. 3, 2022, pp. 1-16.

SANTOS MORÓN, M.J.: "Consumidor y nuevas tecnologías: privacidad y protección de datos", en AA.VV.: *Derecho de consumo: visión normativa y jurisprudencial* (coord. por M.J. SANTOS MORÓN y M.N. MATO PACÍN), Madrid, 2022, pp. 303-321.

SÉNÉCHAL, J.: "Article 16(2) of the 'Digital Content and Digital Services' Directive on the Consequences of Termination of Contract, or the Difficult Articulation between Union Law on Consumer Contract and Union Law on the Protection of Personal Data", en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSE, R. SCHULZE y D. STAUDENMAYER), Nomos/Hart, Baden-Baden (Munich), 2020, pp. 147-162.

SOLOVE, D.J.: "Privacy Self-Management and the Consent Dilemma", *126 Harvard Law Review 1880*, núm. 141, 2013, pp. 1180-1903.

STAUDENMAYER, D.: "Comentario al art. 3 Directiva (UE) 2019/770", en AA.VV.: *EU Digital Law. Article-by-Article Commentary* (dir. por R. SCHULZE y D. STAUDENMAYER), Nomos Verlagsgesellschaft, Baden-Baden (Munich), 2020, pp. 57-91.

TORRE DE SILVA Y LÓPEZ DE LETONA, J.: "El derecho civil de los datos", *Anuario de derecho civil*, vol. 72, núm. 3, 2019, pp. 825-877.

TRIPODI, E.M.: "Consumi digitali e dati personali", en AA.VV.: *I diritti dei consumatori digitali* (dir. por R. TORINO) Pacini Giuridica, Pisa, 2023, pp. 267-290.

VÁZQUEZ-PASTOR JIMÉNEZ, L.: *Contratos de suministro de contenidos y servicios digitales*, Dykinson, Madrid, 2023.

VERSACI, G.: "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *European Review of Contract Law*, vol. 14, núm. 4, 2018, pp. 374-392.

WENDEHORST, C.: "Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?", en AA.VV.: *Data as Counter-Performance – Contract Law 2.0?* (dir. por S. LOHSSE, R. SCHULZE y D. STAUEMANYER), Nomos/Hart, Baden-Baden (Munich), 2020, pp. 193-224.

ZOLL, F.: "Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content", en AA.VV.: *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps* (dir. por R. SCHULZE, D. STAUEMANYER y S. LOHSSE), Nomos/Hart, Baden-Baden (Munich), 2017, pp. 179-188.

