La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)[1]

Digital Contracts and the Loss of Privacy (Between the Data Protection Regulation and the New Directive or the Supply of Digital Contents)

Paloma de Barrón Arniches
Universidad de Lleida
pbarron@dpriv.udl.cat

doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65

Recibido el 23 de mayo de 2019
Aceptado el 17 de junio de 2019.

Resumen: Los datos personales de los usuarios se ponen en circulación con ocasión de la contratación de un bien o un servicio en el mercado digital. El objetivo de estas páginas es analizar esta situación fáctica desde la perspectiva del

---

[1] Trabajo realizado dentro de las actividades de investigación del grupo de investigación consolidado 2017SGR997, reconocido por la Generalitat de Catalunya, y como investigador de los siguientes proyectos: INVID InVID – In Video Veritas, Verification of Social Media Video Content for the News Industry n. 687786, financiado por la Unión Europea; y el proyecto «Retos jurídicos del mercado único digital (MUD): una aproximación desde el análisis económico del Derecho», n.º R/N:L108E3, financiado por la Universidad de Lleida. Quiero agradecer la ayuda inestimable de la becaria de investigación del Departamento de Derecho civil, Dña. Alba Valderrey Fernández.

derecho de contratos, que debe interactuar con el Reglamento (UE) 2016/679 de 27 de abril, de protección de datos. Se dibujan los trazos esenciales del contrato de adhesión para la cesión de datos personales, que los usuarios formalizan en el contexto de la contratación electrónica en el ámbito privado. Se constata que el usuario es la parte débil en el contrato, y que el consentimiento para la cesión de los propios datos no siempre es informado ni libre. Se formulan algunas propuestas para mejorar la posición de la persona física, titular de su información personal.

Palabras clave: Protección de datos, consentimiento del usuario, información precontractual, comercio electrónico.

Abstract: *Users' personal data circulate in the digital market. The purpose of this paper is to analyze this real situation from the perspective of contract law and Regulation (EU) 2016/679 on data protection. The contract of adhesion for the transfer of personal data is formalized in the context of the digital market, and users are the weaker party in the contract, and their consent to the data treatment is not always informed and free. I propose some solutions to improve the position of the personal data owner.*

Keywords: *Data protection, user consent, pre-contractual information, digital market.*

I. **Introducción**

El presente estudio se interesa por la suerte que corren los datos personales de las personas físicas en el devenir del comercio electrónico, especialmente cuando tiene lugar entre empresarios y consumidores (*Business to consumer B2C*). Los datos personales de los usuarios se ponen en circulación con ocasión de la contratación de un bien o un servicio en el mercado digital. Estos datos quedan en poder del empresario, que los analiza y reutiliza para otros fines, básicamente publicidad, que redundará en su mejor posicionamiento en el mercado mediante la obtención de nuevos contratos de compraventa o de prestación de servicios. A través de los datos personales recabados, el empresario —y las empresas terceras con las que está conectado—, conocen al usuario, su perfil como cliente, sus gustos y preferencias y, además, pueden contactar de nuevo con él en cualquier momento.

El objetivo de estas páginas es analizar esta situación fáctica desde la perspectiva del derecho de contratos, porque está claro que la recientemente promulgada normativa sobre protección de datos ha de ser la protagonista[2],

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

pero ¿cómo interactúa con el derecho contractual cuando el trasvase de datos personales se produce con ocasión de un negocio jurídico formalizado digitalmente? ¿Se están produciendo vulneraciones de los derechos de los titulares de los datos? ¿Tiene la persona física la condición de contratante débil con respecto al empresario que recaba la información personal? No tendría por qué ser así, si la cesión de los datos se realiza con pleno conocimiento y consentimiento. El derecho de contratos no debería preocuparse por la justicia sustantiva, y sí solo por garantizar que el contrato sea el resultado de un proceso libre e informado[3]. No obstante, los modernos planteamientos del derecho contractual van más allá y se preguntan sobre este consentimiento, y sobre la justicia del intercambio que se produce en el comercio digital. Hasta qué punto los contratantes titulares de una información personal son realmente conscientes de los derechos o facultades que emanan de esa titularidad[4].

Al respecto, es relevante el valor económico que para el empresario digital representan los datos personales de sus clientes. Cabe preguntarse por

---

personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). En adelante RGPD. Disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016R0679

En cuanto a la normativa nacional, el pasado 7 de diciembre de 2018 entró en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante LOPD, que deroga la anterior LOPD 15/1999, y se adapta al nuevo Reglamento europeo que entró en vigor en mayo de 2018. Cfr. Boletín Oficial de las Cortes Generales, de 6.12.2018., n.º 294. También queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, que se promulgó mientras se tramitaba la LOPD para regular «de urgencia» cuestiones relacionadas con las autoridades de control y la aplicación del procedimiento sancionador previsto en el Reglamento europeo.

[3] Ésta es en esencia la teoría liberal del contrato que, como afirma Gomez Calle, se sustenta en ocasiones en las teorías económicas del contrato. Esther Gómez Calle, *Desequilibrio contractual y tutela del contratante débil*, (Cizur Menor, Civitas, 2018), 22.

[4] ¿Existe un derecho de propiedad sobre los datos personales? ¿es posible convertir los datos personales en objeto de transacción entre las partes, a pesar de su consideración general como derechos de la personalidad? ¿podríamos entender, desde una perspectiva del análisis económico del Derecho contractual, que nos encontramos ante un activo inmaterial susceptible de ser valorado económicamente en el contexto de las prestaciones de las partes de un negocio jurídico privado formalizado por vía electrónica? Estas y otras preguntas son las que se nos plantean con respecto a la noción «titularidad sobre los propios datos personales». Algunos autores ya han empezado a recorrer esta senda: Francisco Javier Puyol Montero, *Aproximación jurídica y económica al Big Data*, (Valencia, Tirant lo Blanch, 2015), 341 y ss.; Luz Martínez Velencoso y Marina Sancho López, «El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?», *InDret* 1 (2018) 6, Ilaria Amelia Caggiano, «A quest for efficacy in data protection: a legal and behavioural analysis», working paper 10/2017, Cátedra Jean Monnet de Derecho Privado Europeo, consultable en http://diposit.ub.edu/dspace/bitstream/2445/113463/1/WP_2017_10.pdf, Última consulta, 4.4.19.

la onerosidad de las transacciones en las que el proveedor no recibe dinero sino solo datos personales, caso que se repite con cierta frecuencia cuando lo que es objeto de transacción es un contenido digital[5]. En estas relaciones jurídicas sin contraprestación dineraria, ¿qué estándares de obligaciones para el proveedor, se pueden aplicar? ¿qué remedios jurídicos tiene el consumidor cuando el proveedor incumple sus obligaciones? Y, en general, en todas las transacciones electrónicas ya se produzca el pago de un precio en dinero o no, ¿qué pasa con los datos personales de los usuarios una vez concluido el negocio jurídico? (por ejemplo, en un contrato de compraventa porque este se consume con la entrega del producto, o en un contrato de suministro de contenidos digitales, porque el consumidor puede decidir poner fin al contrato en cualquier momento). No debe olvidarse que el respeto y la protección de la privacidad de los usuarios también constituye una condición para el desarrollo de los mercados digitales e, incluso, un motor de innovación, ya que los bienes y servicios de la economía de datos solo serán aceptados por los consumidores si se respeta esta preocupación por su privacidad y confidencialidad[6].

En definitiva, cabe preguntarse si en el ámbito del comercio electrónico no se está produciendo un cierto e importante desequilibrio entre los contratantes, incluso hasta alcanzar situaciones de clara arbitrariedad. En efecto, en la relación contractual electrónica el usuario persona física que pierde su privacidad se encuentra en una posición de debilidad que es aprovechada conscientemente por el empresario que recaba y trata los datos de sus clientes, exclusivamente en su propio beneficio. Como ha señalado algún autor, el Derecho contractual debe adaptarse al mundo digital, manteniendo la continuidad de los conceptos clave, —como lo es el equilibrio entre las prestaciones y la protección a la parte más débil en el contrato—, y combinándolos con los enfoques innovadores respecto a las nuevas tecnologías y prácticas empresariales[7], esto es, en definitiva, am-

[5] Véase la 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, publicada en el Diario Oficial de la Unión Europea el 22 de mayo de 2019 (L136/1), esto es, un día antes de la entrega de este trabajo a la revista. Advierte el autor que el trabajo de investigación se ha realizado, por tanto, sobre la base de la Propuesta de Directiva, que se presentó el 9.12.2015, cuyo contenido, en gran medida, se ha visto confirmado en el vigente texto legal europeo.

[6] Josef Drexl. «Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC», consultable en https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf. Última consulta, 4.4.19.

[7] Reiner Schulze. «Contratar en la era digital», working paper 8/2018, Cátedra Jean Monnet de Derecho Privado Europeo, 11, consultable en http://diposit.ub.edu/dspace/handle/2445/124048 Última consulta, 4.4.19. Insiste este autor en señalar: *«El contrato*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

pliando el ámbito de aplicación de estos principios básicos del Derecho de contratos.

II. **Los datos y su rol dentro de la economía digital**

La información relativa a los usuarios de internet, las personas físicas, constituye un activo intangible que tiene un reflejo contable en la empresa en tanto que generará beneficios económicos futuros, controlados por la entidad[8]. De hecho, la pregunta sobre el valor económico de la información parte de la constatación de todo lo que el empresario puede realizar a partir de los datos de sus clientes. Gracias a la visualización de información personal se pueden descifrar datos complejos y explorar visualmente información relevante de las personas de forma inteligente, rápida y sencilla. Así, una empresa mediana de servicios puede descubrir nuevas formas de satisfacer a los clientes, un organismo gubernamental puede predecir dónde resultan más necesarios sus recursos: organizaciones de todos los tipos y tamaños emplean la visualización de datos para mejorar las relaciones con los clientes, combatir el fraude y mucho más: todos toman mejores decisiones gracias al fácil acceso a una analítica potente e interactiva, el llamado Big Data[9]. En concreto, los proveedores digitales mejoran su posicionamiento de mercado, actualizan su oferta conforme a las nuevas necesidades y tendencias del mercado, identifican nuevos nichos de negocio que les permiten diversificarse y crecer. La información personal se ha convertido en un factor de competencia para las empresas, descrito como una «materia prima para los modelos de negocios digitales». Se utiliza para determinar tendencias y comportamientos estacionales, simular escenarios económicos, segmentar clientes, prevenir sus de-

---

es el instrumento jurídico más importante para una economía de mercado. Sin Derecho contractual, una economía de mercado no puede funcionar. Por lo tanto, la pregunta central para todos nuestros países es cómo adaptar el Derecho de la contratación al mundo digital» (5).

[8] *«(…) se debe impulsar una mayor promoción del tratamiento contable de los activos intangibles, la protección de los registros de propiedad intelectual, y el apego a las normas de información financiera, como parte de un marco legal que le asigna un mayor valor monetario a los activos intangibles»* (200), «Estudio sobre el valor económico de los datos personales», entregable final elaborado por la organización CLUSTERTIC, de la Universidad de Colima, México, consultable en http://clustertic.org/wp-content/uploads/2016/06/valor_eco_Datospersonales_FINAL.pdf. Última consulta, 4.4.19.

[9] Se define el Big Data como el almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de internet. Luz Martínez y Marina Sancho, «El nuevo concepto de onerosidad en el mercado digital» *op.cit.,* (14).

cisiones[10]. A partir de esta información, las empresas pueden mejorar los propios productos y la publicidad. El resultado es un evidente aumento de los beneficios empresariales.

Estamos hablando, en efecto, de un gran volumen de datos, no solo de los datos de un individuo sino de los de millones de ellos. Esto es lo que está haciendo ricos a los proveedores digitales, sin embargo ¿Quién regula la obtención y utilización de esos grupos de datos, de esos perfiles automatizados? Si se analiza el Reglamento Europeo de Protección de datos se puede constatar que esta normativa de Derecho público, si bien regula la recopilación y el procesamiento de los datos personales de cada individuo, no proporciona mecanismos eficaces para controlar el uso que de las tecnologías de elaboración de perfiles llevan a cabo las empresas. Hay pocos instrumentos en manos de los ciudadanos para conocer y decidir sobre la forma en que se utilizan sus datos, una vez cedidos al proveedor. Las decisiones basadas en tratamientos automatizados de datos se recogen en el Reglamento, pero con una definición amplia y, únicamente, en línea de principios[11]. Lo mismo ocurre en la reciente norma española[12]. Además, el consumidor difícilmente dispondrá de los conocimientos y de los medios técnicos para poder realizar, de facto, ningún control sobre los datos que transfiere, su utilización posterior y su posible transmisión a terceros. Tampoco es factible que las autoridades de control puedan realizarlo respecto de todos los proveedores digitales que operan en el mercado, ni tan siquiera en el europeo. Aún más, el problema más grave es la propia tecnología, puesto que hoy día difícilmente puede hacerse desaparecer completamente la información personal que se sube a internet[13].

---

[10] Así lo explica Ilaria Amelia Caggiano: *«Value extraction in big data takes place through analytical methods of data mining (algorithms). Analytics are data tracking tools: software that lets you find correlation between data, analyse historical series, determine trends and seasonal behaviours, simulate economic scenarios, segment customers, and conduct data and text mining activities to better understand a wide range of phenomena Of business. These are tools that enable private and public decision-makers to make better decisions. Providing budget indicators based on historical series, understanding customers and employees' behavior in advance, assessing the degree of risk of funding, are some practical examples of analytics use»;* «A quest for efficacy in data protection…», *op. cit.* (4); veáse también Susana Navas Navarro, «El almacenamiento de los datos: del cloud computing al AND sintético» en *Mercado digital. Principios y reglas jurídicas,* ed. por *idem*, (Valencia, Tiranch lo Blanch, 2016), 63-90.

[11] En efecto, el Cdo. N.º 72 del Reglamento señala que *«La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto».* En el siguiente apartado trataré más en detalle esta cuestión.

[12] Arts. 18, 28 y 34 LOPD.

[13] Afirma Marina Sancho: *«A pesar de que el nuevo Reglamento Europeo comprende novedades interesantes y goza de buenas intenciones, lo cierto es que la tecnología en sí*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

Así las cosas, las empresas publican políticas de privacidad, pero el cumplimiento de estas políticas casi nunca se prueba. En caso de violaciones de derechos de los ciudadanos, que se manifiestan a través de reclamaciones individuales, la autoridad de protección de datos solo puede intervenir y tomar medidas para resolver esas situaciones individuales, no el conjunto del *modus operandi* de las empresas digitales, las cuales, para empezar, ni siquiera reconocen o contabilizan en su haber estos activos inmateriales consistentes en los bancos de datos que constantemente les proporcionan sus propios clientes. Protegidas por la desregulación y el desconocimiento que rodea a las nuevas tecnologías de tratamiento de la información, las empresas prefieren no evaluar el impacto económico que para ellas se deriva de esta cesión gratuita de datos que reciben de una forma continuada en el desarrollo de su negocio.

Ahora bien, es necesario matizar que los datos personales no generan valor y riqueza meramente por su transformación en información; sino que su valor se genera por su participación en un proceso de creación o transformación de productos y servicios[14]. Por tanto, desde una perspectiva económica será un dato relevante la capacidad de los proveedores de internet, de cada empresario de la economía digital, de asumir estos procesos de transformación de los datos de sus usuarios en nuevo conocimiento. A nivel internacional no se cuenta con un modelo reconocido para estimar el valor monetario de los datos personales, ni con una medición del impacto del valor de los datos en las empresas en los diversos sectores de actividad económica y, en último término, en el producto interior bruto de cada Estado. Sin embargo, los economistas trabajan en esta materia, tratando de obtener siquiera sea de manera indiciaria, algunas conclusiones[15].

---

misma constituye una limitación para el cumplimiento total de los derechos que allí se comprenden pues, por ejemplo, hasta la fecha no hay manera posible desde un punto de vista técnico de borrar por completo y para siempre la información subida a Internet.» («El nuevo concepto de onerosidad… *op. cit.*, p. 17). Véase también Susana Navas Navarro, «Cookies y tecnología análoga: publicidad comportamental online y protección de datos de carácter personal» en *Mercado digital op. cit.*, 357-380.

[14] Es lo que se denomina economía basada en el conocimiento: formas, métodos, herramientas o medios de producción para abordar y resolver problemas, producir un mayor conocimiento y así, diseñar productos y servicios mejores. «Estudio sobre el valor económico de los datos personales», *op. cit.,* 119 y ss.

[15] Pueden consultarse, entre otros los siguientes análisis económicos sobre esta materia: «Unleashing the value of consumer data», 2013, consultable en https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_unleashing_value_of_consumer_data/; «Rethinking personal data: A New Lens for Strengthening Trust» consultable en https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/wef-rethinking-personal-data-new-lens-strengthening-trust; «Data Brokers. A call for transparency and Accountability», Federal Trade Comission, 2014. Consultable en https://www.stopdatamining.me/data-brokers-transparency-accountability-ftc-report-2014/ Última consulta, 4.4.19.

Puede destacarse, por ejemplo, un estudio realizado a partir de una muestra obtenida mediante encuestas a un amplio espectro de personas físicas y a un amplio espectro de empresas. El objetivo era determinar el valor económico que para las personas tiene su privacidad, y el valor económico que los empresarios atribuyen a la información recibida de sus clientes. Respecto a las personas físicas, una interesante conclusión obtenida por estos estudios es que siempre es más alta la cantidad que los ciudadanos estarían dispuestos a recibir por la venta de sus datos personales que la que estarían dispuestos a pagar por su protección[16]. En segundo lugar, se confirma que los individuos participantes con nivel educativo universitario o posgrado son los que muestran un mayor valor monetario en el promedio de sus registros, seguido de los participantes con carreras técnicas y, finalmente, los participantes con niveles educativos inferiores. Esto puede llevarnos a inferir que conforme sea más elevado el nivel educativo, mayor será el valor que el individuo asignará a sus datos personales, es decir, a su privacidad[17]. Por otro lado, los datos personales considerados no sensibles son lo que muestran una mayor aportación al valor monetario total de la información privada de los individuos. Específicamente los datos de identificación y contacto, y los datos financieros y patrimoniales, son los más valiosos desde la perspectiva de los individuos participantes[18]. Por referencia a las entrevistas realizadas a empresas, concluye el estudio analizado que los datos de identificación y contacto son de los más importantes para las empresas encuestadas (especialmente el dato del correo electrónico, el teléfono particular y el nombre, por ese orden)[19]. Por tamaño de empresa, se puede observar que las empresas medianas y grandes son las que otorgan un mayor valor monetario, en promedio, tanto al registro de datos como al valor de cada dato individual, seguido de las pequeñas, y finalmente las microempresas[20].

---

[16] «Estudio sobre el valor económico de los datos personales» *op. cit.*, 146. Por otra parte, en la página web http://www.totallymoney.com/personal-data/ mediante la realización de un test, se puede comprobar la diferencia entre el valor que cada uno le otorgamos a nuestra información personal más básica y el valor real por el que una empresa anunciadora pagaría por ella. Última consulta, 4.4.19.

[17] «Estudio sobre... *op. cit.,* 150.

[18] «Estudio sobre... *op. cit.,.,* 135 y 140.

[19] «Estudio sobre… *op. cit.,.,* 164.

[20] Ello resulta coherente con la mayor capacidad de las empresas grandes de aplicar una economía basada en el conocimiento de esta información personal: *«Con relación a las razones financieras obtenidas, se obtuvo que en promedio los gastos de operación de las empresas participantes representan el 38.36% de sus ventas brutas del último ejercicio fiscal, y los costos asociados al tratamiento de datos personales representan el 13.1% de los gastos de operación de las empresas (Tabla I.53). En este sentido, los costos asociados al tratamiento de datos personales representan el 6.2% de los gastos de operación de las*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

En conclusión, se puede afirmar que en la actualidad existe un modelo de negocio basado en la utilización y explotación de la información personal de las personas físicas, el Big Data genera negocio, es un mercado que funciona y cuyos ingresos son cada día mayores, en proporción inversa a lo que ocurre con la privacidad y la seguridad jurídica de los individuos en la red, que día a día disminuye. Estos usuarios ceden, se supone voluntariamente, sus datos personales, pero, paradójicamente, no se ven repercutidos económicamente, en absoluto. Es necesario sopesar qué papel juega en todo esto el Derecho[21], qué mensajes lanza al mercado la actual legislación relativa a la privacidad y también, por qué no, el moderno Derecho de contratos, todo ello a los efectos de mejorar, si es posible, la posición de los consumidores con respecto a las empresas que comercializan con su información personal.

III. **La protección jurídica de los datos personales**

1. *Ejes de la normativa europea y española de protección de datos*

El fundamento de la protección que el derecho otorga a los datos personales es el concepto de intimidad y de privacidad[22]. En España encuentra su origen y fundamento en la dicción del artículo 18 de la Constitución Española (en adelante CE), que en su apartado 4 concreta que «*La ley limitará el uso de la informática para garantizar el honor, la intimidad perso-*

---

empresas, y las ventas brutas asociadas al uso de datos personales representan el 22.6% de las ventas de las empresas participantes» («Estudio sobre… *op. cit*., 176).

[21] *«Las normas jurídicas constituyen incentivos o desincentivos a los efectos de que sus destinatarios realicen o dejen de realizar tales actividades. La gente, en términos agregados, reacciona de manera distinta según sea el contenido y la naturaleza de las normas (leyes, reglamentos, doctrinas jurisprudenciales, etc.) que regulan su comportamiento»* Gabriel Domenech Pascual, «Por qué y cómo hacer análisis económico del Derecho», *Revista de administración pública*, (2014), 195, 102.

[22] La definición de la Real Academia Española de la lengua, del término privacidad es la siguiente: *«Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión»*. Lo cierto es que este término solía emplearse más en la tradición jurídica del *common law* que en la nuestra, si bien su generalización es una buena noticia para las personas físicas, por cuanto resalta la idea de que, si bien los datos personales no forman parte de nuestra intimidad, sí que afectan a nuestra esfera privada y deben ser objeto de protección jurídica. Entre la doctrina puede consultarse, Lucia Ruggeri, «La tutela de los datos personales en los contratos de la sociedad de información» en *Contratación electrónica y protección de los consumidores. Una visión panorámica* ed. por Leonardo B. Pérez Gallardo, *(*Zaragoza, Reus, 2017), 17-49; Concepción Conde Ortíz, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad,* (Madrid, Dykinson, 2005), especialmente páginas 23-26; Alberto de Franceschi, *La circolazione dei dati personali tra privacy e contratto,* (Napoli, Edizioni Scientifiche italiane, 2017).

nal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». A partir de ahí, su configuración como derecho independiente respecto del derecho a la intimidad ha sido obra del Tribunal Constitucional, que lo ha ido desligando de la protección de la Ley Orgánica 1/1982 para encontrar su ámbito específico de protección[23]. Es relevante, en primer lugar la Sentencia del Tribunal Constitucional 254/1993[24], en la que se define por primera vez el llamado «derecho a la libertad informática», y también la Sentencia 292/2000[25], en la que se remarca su existencia independiente respecto del derecho a la intimidad, definiendo el derecho a la protección de datos como la potestad de control del individuo sobre sus datos personales[26].

En cuanto a la legislación ordinaria, y tras el periodo de transición que se ha vivido en nuestro país hasta el pasado 6 de diciembre de 2018, disponemos de la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que supone la adaptación de la norma española al ahora ya vigente Reglamento europeo General de Protección de datos. El artículo 1.a) de esta Ley expresamente establece que: *«El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica»*. Así pues, la protección a las personas físicas en materia de datos personales se va a garantizar en España por la doble aplicación tanto del derecho interno como del Reglamento europeo, de aplicación directa en todos los Estados de la Unión.

Se pueden identificar y poner en relación con la práctica negocial *on line* de los consumidores, los siguientes principios rectores de la protección de datos presentes en el Reglamento europeo[27] y en la LOPD, principios que, a su vez, se traducen en diversas obligaciones para los responsables del tratamiento de los datos:

1. Principio de lealtad y transparencia en el tratamiento de los datos de las personas físicas: art. 5.1.a) RGPD. Estos dos principios están muy inter-

---

[23] LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen [BOE núm. 115, de 14/05/1982].

[24] STC 254/1993 de 20 julio, RTC\1993\254.

[25] STC 292/2000 de 30 noviembre, RTC\2000\292.

[26] STC 292/2000, FJ 6: *«Derecho fundamental a la protección de datos: el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer los derechos fundamentales enumerados en el art. 18.1 CE (…) persigue garantizar un poder de control sobre sus datos personales y sobre su uso y destino con propósito de impedir su tráfico ilícito y lesivo»*.

[27] Lukas Feiler, Nikolaus Forgó, Michaela Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary,* (Surrey, German Law Publishers, 2018).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

conectados entre sí, y conducen directamente a las obligaciones de información sobre el destino y la utilización que piensa darse a los datos personales recabados en el momento de la celebración de un negocio jurídico. La transparencia del proveedor de internet, de la empresa con respecto al consumidor que solicita el bien o servicio, constituye el presupuesto para el ejercicio por parte de éste, de todos sus derechos[28]; es el sistema de doble capa de protección de datos. Se debe poner a disposición del usuario información básica sobre cómo se van a tratar sus datos personales con ocasión de cada uno de los formularios en los que el usuario tenga que facilitar sus datos personales. Esta primera capa debe enlazar con la información completa sobre la política de privacidad de la empresa, o segunda capa de la protección de datos.

2. Principio de exactitud y minimización de datos: artículo 5.1.c) y d) RGPD. Los datos serán exactos y, si fuere necesario, actualizados. Si no fuera así, deberá procederse a su rectificación o eliminación. Junto a ello, la minimización significa que únicamente deben requerirse y obtenerse los datos de la persona física que resulten necesarios en cada caso[29]. Los datos personales tienen que ser los adecuados y pertinentes en relación con las finalidades para las cuales son recabados. Hay que considerar que puede precisarse diferente información personal en los negocios jurídicos concertados por vía electrónica, por ejemplo, la compraventa de bienes corporales no exige más datos que los meramente identificativos y los necesarios para el pago del precio, mientras que el suministro de contenidos digitales puede implicar la necesidad de recabar más datos para hacer posible el ejercicio continuado de los servicios postventa, o el mantenimiento de la situación de conformidad de los contenidos digitales durante todo el tiempo que se prolongue el suministro (por ejemplo, la localización geográfica del consumidor cuando este dato sea necesario para saber si una aplicación móvil podrá funcionar correctamente, o para poder proporcionar las actualizaciones o reparar el software, si fuera necesario). El principio de minimización de los datos también entra en relación con el de conservación de los mismos, de modo que el Reglamento limita el plazo de conservación de la información en poder del proveedor o empresario, y le obliga a informar al titular de los datos sobre esta cuestión. Si no es posible fijar un plazo, sí deberá al menos establecer los criterios que permitan determinar el plazo de conservación[30].

---

[28] Arts. 12-15 RGPD, en concordancia con lo dispuesto en el art. 11 LOPD. Debe concederse que la norma es cuidadosa y exhaustiva a la hora de determinar los aspectos sobre los que recae el deber de información del responsable del tratamiento.

[29] Aunque referida a la normativa española anterior (Ley 15/1999) véase Pedro Alberto de Miguel Asensio, *Derecho privado de internet*, (Cizur Menor, Civitas, 2015) 315 y ss.

[30] Art. 5.1. e), en concordancia con el 13.2.a) y art. 14.2.a) RGPD.

3. Deber de integridad y confidencialidad con respecto a los datos recabados: art. 5.1 f) RGPD. Afecta a responsables y encargados del tratamiento de datos, así como a todas las personas que intervengan en cualquier fase de éste. Configura una obligación general que resulta complementaria de los deberes de secreto profesional que afectan a los empresarios o prestadores de servicios, en función del ámbito de su actividad profesional. La confidencialidad que afecta a los datos recabados también implica la adopción de medidas técnicas y de organización que permitan asegurar la conservación y la no transmisión de estos datos a terceros sin permiso de su titular: la responsabilidad de quien los recaba alcanza la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

4. Responsabilidad proactiva del encargado o responsable del tratamiento de datos con respecto al cumplimiento de sus obligaciones como tal. Expresada en el apartado segundo del art. 5 RGPD, constituye el colofón de este elenco de protecciones al ciudadano, titular de su propia privacidad. El encargado y el responsable deben estar en todo momento preparados para cumplir sus obligaciones y para poder probar dicho cumplimiento. En términos procesales significa que recae sobre estos dos sujetos la carga de la prueba de haber adoptado todas las medidas necesarias para que los principios anteriormente expuestos sean una realidad. Se trata, en definitiva, de rendir cuentas sobre cómo se efectúa el tratamiento[31] poder probar que se ha adoptado una política de protección de datos (que se registran las operaciones de tratamiento, se establecen y siguen ciertos códigos de conducta, se adoptan medidas de seguridad revisables de forma periódica etc.). Así mismo, dentro de esta responsabilidad proactiva se incluye el deber de notificar las violaciones de la seguridad de la información que, en el ejercicio de las propias funciones, puedan detectarse.

Qué duda cabe que este ejercicio de la responsabilidad proactiva en la protección de los datos por parte del empresario o el proveedor de servicios *on line* coloca en una posición segura al consumidor. Sin embargo, la realidad es otra por varios motivos: primero, porque no toda la normativa de protección de datos es tan exigente como podría desprenderse de la lectura de lo expuesto hasta aquí. Por ejemplo, es mucho más dudosa la regulación relativa a la elaboración de perfiles con fines comerciales, y también resultan ambiguos los criterios que identifican en determinados casos, la licitud del tratamiento de datos personales. En segundo lugar, no está tan clara la manera en que el consumidor puede verificar este comportamiento proac-

[31] Para lo cual el responsable puede dotarse de las herramientas que están previstas en el capítulo IV del RGPD, véase art.25 y concordantes.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

tivo del empresario, ni tampoco la eficiencia de las fórmulas previstas para restablecer sus derechos cuando estos resulten vulnerados[32].

Respecto a la regulación sobre elaboración de perfiles, el art. 4., apartado 4) incluye en este concepto *«toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física»*. Este amplio y efectivo seguimiento y control de los comportamientos *on line* de los usuarios resulta, así, admitido por el legislador europeo bajo el paraguas de una previa información al interesado a que hacen referencia los arts. 13 y 15 RGPD. Sin embargo, no es muy defendible entender que este seguimiento exhaustivo de comportamientos y preferencias encaje realmente con el criterio de minimización de la información personal que se puede recabar. El empresario realmente no *necesita* esta información para desarrollar su negocio, lo que ocurre es que la tecnología le permite acceder a ella y accede, porque su análisis le produce beneficios económicos relevantes[33].

---

[32] Stéphanie Van Gulijk *et al*.., «Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach», *European Review of Private Law* 5 (2018), 635-660. Insisten estos autores en que la normativa legal de protección de datos, basada en el derecho público no es eficiente para proteger al titular de los datos. La legislación pública europea está dotada de pocos instrumentos para mejorar el control por parte de los ciudadanos sobre la forma en que se utilizan sus datos.

[33] La monitorización de las conductas en internet se realiza a través de las cookies y otras tecnologías de recogida automática de datos. Veamos un ejemplo: los datos que recoge automáticamente un proveedor de contenidos digitales, sin que el usuario realice más comportamiento activo que el consistente en clicar en ACEPTO (la política de cookies de esta página web), dado que en la página no se muestra la opción contraria (RECHAZO la política de cookies de esta página web) sino que, si el usuario no quiere aceptar debe clicar en MAS INFORMACIÓN, y navegar por un sinfín de informaciones y normas de funcionamiento de la página, de las que tendrá que extraer la información sobre cómo impedir que su navegación implique el consentimiento tácito al proveedor para que utilice cookies. Y así, la web de una empresa americana que se declara sujeta a las reglas del Escudo de Privacidad, expone que recopila automáticamente la siguiente información del usuario: *Dirección IP; Identificadores del móvil o de otros sistemas o dispositivos; Información relativa al navegador, como tipo de navegador o idioma preferido; Páginas de referencia y de salida, además de las páginas de aterrizaje y las páginas visualizadas; Tipo de plataforma; Información sobre sus dispositivos, hardware y software, como por ejemplo la configuración y los componentes de su sistema, los programas y actualizaciones de EA que haya instalado o utilizado y la presencia de los complementos necesarios; Información sobre los productos de EA que utiliza y el uso que hace de los mismos; Información sobre eventos de los dispositivos, como por ejemplo informes de fallos, URL solicitadas y remitidas e información sobre la actividad del sistema…»*

Ante esta situación, las opciones para el ciudadano son dos, o bien consentirlo sin pararse en exceso a sopesar el valor de su privacidad ni los perjuicios de perderla, o bien oponerse a este tratamiento de la información que él mismo ha proporcionado, mediante el ejercicio del derecho de oposición que prevé el art. 21 RGPD, al que expresamente se remite el vigente art. 18 LOPD. El art. 21 RGPD, en su apartado 3 ordena que el responsable del tratamiento deje de tratar esos datos personales del usuario para fines de *mercadotecnia*, o marketing, pero, ¿cómo puede controlarse que, en efecto, lo haga?, y aunque quisiera hacerlo, ¿puede el responsable, tecnológicamente hablando, hacer desaparecer de internet los datos personales ya recabados al usuario?[34].

En segundo lugar, está la cuestión de la licitud o los intereses legítimos que justifican el tratamiento de datos personales. El principio de licitud del tratamiento se enuncia en el art. 5.1. b) RGDP, y se desarrolla en el art. 6, por su importancia para legitimar todas las actuaciones del responsable del tratamiento. Antes, en el Cdo. 47, el Reglamento especifica que el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo, y lo hace después de una larga disquisición, que podría calificarse de vaga y algo teórica, sobre la contraposición entre estos denominados intereses legítimos y los intereses o los derechos y libertades de los ciudadanos[35]. A partir de aquí, cabe concluir que el consentimiento del interesado deja de ser el

[34] Véase nota 13.

[35] *Cd. 47: «El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo».*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

único requisito clave y que, incluso en ciertos casos, podría considerarse prescindible[36].

Por último, debe considerarse que la mayoría de empresas proveedoras de bienes y servicios *on line* son americanas, el intercambio de datos entre los EE.UU y la UE es el más elevado que existe a nivel mundial, y es de sobra conocido que la protección a la privacidad es escasa en la legislación de los EEUU. Ahora bien, respecto a los datos transferidos para fines comerciales está vigente en la actualidad el llamado Escudo de la privacidad UE - EE.UU, que fija normas para los flujos de datos transferidos entre empresas de ambos continentes con fines puramente comerciales[37]. Por su parte, el vigente RGPD se refiere expresamente a su aplicación a los proveedores de servicios de la sociedad de la información que no tienen sede en la UE, pero que manejan datos de ciudadanos europeos, en concreto estableciendo la obligación del proveedor de nombrar un representante que tenga sede en el territorio en la Unión[38]. Sin embargo, la tendencia de sobra conocida de las empresas americanas es la de extender su modelo de negocio a todo el mundo tratando de prestar sus servicios en los mismos términos a escala global. Esa opción, en la medida en que los términos contrac-

---

[36] Art. 6.1,f) RGPD.

[37] C (2016) 4176 final, «Commission Implementing Decision of 12.7.2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield». Consultable en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=EN Última consulta, 5.4.19.

[38] Art. 3.2 y art. 27 RGPD. También es significativa, a los efectos de poder entender la voluntad claramente protectora de la Unión Europea respecto a la privacidad de sus ciudadanos, la Sentencia del Tribunal de Justicia: asunto C-362/14, Schrems y Data Protection Commissioner versus Digital Rights Ireland Ltd., Sentencia de 6 de octubre de 2015 El Tribunal se pronunció con respecto a la posibilidad de un Estado miembro de decidir si es ajustada a Derecho la transferencia de determinados datos personales desde dicho Estado a un país tercero, en función del nivel de protección de la privacidad que se de en ese país tercero, todo ello a la luz de la entonces vigente Directiva 95/46, con cita de alguno de sus Considerandos principales: *«Cdo. 56 […] los flujos transfronterizos de datos personales son necesarios para [el] desarrollo del comercio internacional; […] la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; […] el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias. Cd. 57: […] por otra parte, […] cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales»* El país tercero en este caso, obviamente, era EEUU. Puede consultarse esta resolución en http://curia.europa.eu/juris/document/document.jsf;jsessionid=8B3C6F365A493BCD920BE7DD21B2AB86?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2990 Última consulta, 5.4.19.

tuales puedan no estar adaptados al nivel de protección que deriva de la legislación europea plantea obvios riesgos legales o, dicho de otra manera, reclama una eficaz tutela de los derechos de los usuarios conforme a los estándares de la UE[39].

2. *La tipología de los datos personales y los diferentes niveles de protección*

2.1. Datos no sensibles y categorías especiales de datos

Los principios básicos de protección a la privacidad de las personas se aplican, como es bien conocido, en diferente medida en función de la tipología de los datos personales que son objeto de tratamiento. Así pues, y con respecto a la contratación electrónica con consumidores, cabe considerar en primer lugar cuál es la información personal, qué tipología de datos personales requiere el proveedor digital de bienes y servicios y, por tanto, qué está autorizado a recabar de la persona física que desea contratar. El acercamiento a esta materia permite determinar con más precisión el nivel de protección que la norma ofrece a los consumidores (los interesados, según los denomina el RGPD).

El concepto de datos de carácter personal, se encuentra definido en el art. 4.1 RGPD como *«toda información sobre una persona física identificada o identificable»*. Resulta indiscutible que sin datos del cliente no hay contrato electrónico, ni de compraventa ni de servicios, ni ningún otro. Los datos necesarios para el comercio electrónico son los que los analistas identifican (por el valor que los propios usuarios les atribuyen), como datos no sensibles[40]. Pero lo cierto es que los objetivos de negocio de las

---

[39] Así, señala Pedro de Miguel: *«la aplicación a este tipo de situaciones del artículo 6 RRI será determinante para apreciar que, la previsión en las condiciones generales de que la ley aplicable es la del Estado de California no puede acarrear que el consumidor se vea privado de la protección que le proporcionan las normas imperativas de la legislación española, como es el caso de las contenidas en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (de conformidad también con lo previsto en el art. 67 TRLGDCU). Entre esas normas imperativas se encuentran las relativas a las condiciones generales y cláusulas abusivas, un ámbito sustancialmente armonizado en el marco europeo desde la adopción de la Directiva 93/13/CEE, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores»*. Blog de Pedro de Miguel Asensio, entrada de 24.5.2012, consultable en http://pedrodemiguelasensio.blogspot.com/2012/05/facebook-y-proteccion-de-los.html.

[40] Véase el trabajo de campo que se realiza en «Estudio sobre el valor económico de los datos personales», *op. cit.*,135-137: *Los datos no sensibles se dividen en seis (6)*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

empresas que trabajan en el sector privado *on line,* van mucho más allá de la mera venta de sus productos, lo que buscan es elaborar, mientras realizan sus transacciones electrónicas, verdaderos estudios de mercado. Para ello, manejan dos tipos de información sobre sus clientes, la primera que podría considerarse información real derivada de los datos concretos proporcionados por estos (nombre, lugar de residencia, profesión, estado civil, teléfono de contacto, correo electrónico), y la segunda información obtenida a través de otros parámetros como son las pautas de comportamiento, preferencias culturales o patrones de consumo. Ambos tipos de información quedan almacenados en enormes bases de datos, y unos y otros permiten identificar o reconstruir la identidad de cada usuario atribuyéndole una información sobre su religión, ideología, clase social, salud, que puede o no ser cierta —cuestión extremadamente relevante—, por cuanto no proviene de datos objetivos cedidos al proveedor, sino que se obtiene mediante la triangulación y organización de la información real obtenida de cada individuo.

Por tanto, a través de los tratamientos automatizados y la elaboración de perfiles y partiendo de datos no sensibles proporcionados por los usuarios, las empresas digitales de una cierta magnitud son capaces de llegar —siquiera sea de forma presunta— a los datos que son considerados por los propios ciudadanos y también por el legislador, como datos de categoría especial[41], o datos sensibles (origen étnico o racial, convicciones religiosas o filosóficas, vida sexual etc.). Es ahí donde las personas físicas han perdido la batalla, primero porque al permitir la creación de perfiles automatizados autorizan la pérdida total y absoluta de su privacidad sin apenas ser conscientes de estar haciéndolo; y segundo porque la tecnología los «encasilla» en modelos estándar de personas de un estrato socioeconómico determinado, un grupo que responde a los mismo patrones predeterminados de comportamiento, patrones que sirven de guía al mercado y, al mismo tiempo, permiten que se impulse a la ciudadanía hacia unos hábitos de consumo cada vez más estandarizados.

---

subgrupos o familias de datos: 1) Identificación y Contacto, 2) Laborales, 3) Académicos, 4) Entretenimiento, 5) Migratorios, y 6) Financieros y Patrimoniales (…). En los datos de identificación y contacto se obtuvo un promedio de 7.8, donde la firma electrónica es el dato calificado más valioso con 9.2 (en una escala de 0 – 10), seguido de la firma autógrafa (9.1) y los datos de domicilio (9.1), situándose muy por encima del promedio (Gráfica 1.38). Les siguen en importancia los números telefónicos, tanto el teléfono particular como el número del teléfono móvil de los individuos participantes. Los datos de identificación más comunes como edad, nacionalidad y estado civil son los considerados de menos importancia (..) entre los Datos No Sensibles, los datos financieros o patrimoniales son los que significaron una mayor importancia para los individuos participantes con una calificación promedio de 8.7».

[41] Art. 9 RGPD.

2.2. Los datos como contraprestación de determinados servicios digitales

En este contexto, conviene recordar la recientísima normativa europea sobre contratos de suministro de contenidos digitales, en la que expresamente se contemplan los datos personales como la contraprestación que ha de pagar el usuario para recibir determinados servicios digitales[42]. Si el proveedor de servicios va a tratar los datos del usuario —por ejemplo, con fines de marketing—, entonces la revelación de información personal por parte de éste se considera contraprestación y el negocio jurídico cae dentro de la órbita de aplicación de la Directiva, cuya finalidad es garantizar los derechos de los consumidores, especialmente su derecho a la conformidad de los contenidos digitales adquiridos[43]. Este planteamiento supone un importante avance, puesto que convierte el trasvase de datos personales en una parte del contrato y, por tanto, sujeto a las normas del derecho contractual, no solo a la normativa general de protección de datos.

Así pues, el negocio jurídico aborda, como una única propuesta contractual a la que se adhiere el usuario, la prestación de un servicio digital a cambio de la cesión de datos personales. La contraprestación del usuario consiste precisamente en el permiso para la utilización de tecnologías de creación de perfiles automatizados, porque además de los datos de identificación se le requiere también el permiso para esta finalidad, bajo la advertencia de que, en caso de no concederse tal autorización, el proveedor no podrá prestar el servicio[44]. Además, esta situación se produce también

---

[42] Art. 3.1 Directiva 2019/770 : *«La presente Directiva también se aplicará cuando el empresario suministre o se comprometa a suministrar contenidos o servicios digitales al consumidor y este facilite o se comprometa a facilitar datos personales al empresario, salvo cuando los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales con arreglo a la presente Directiva o para permitir que el empresario cumpla los requisitos legales a los que está sujeto, y el empresario no trate esos datos para ningún otro fin.»*

[43] Sergio Cámara Lapuente, «El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015», *InDret* 3 (2016), (http://www.indret.com/pdf/1242.pdf).

[44] El ejemplo paradigmático es Google, empresa norteamericana de servicios digitales por internet, que se declara sujeta a las reglas del Escudo de Privacidad. El texto literal sobre privacidad reza así: *«Utilizamos cookies propias y de terceros para mejorar la experiencia de navegación, y ofrecer contenidos y publicidad de interés. Al continuar con la navegación entendemos que se acepta nuestra Política de cookies»*. Por tanto, el hecho de seguir navegando se convierte en un consentimiento tácito para la monitorización de sus búsquedas y actividades en internet, luego esa es la manera que tiene el usuario de pagar la contraprestación por el servicio, porque si después desea cambiar la configuración del navegador y desactivar las cookies, automáticamente se desactivan algunos servicios «gratuitos», tales como el traductor automático o el correo Gmail.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

cuando el consumidor paga un precio por el servicio digital, en ambos casos se ve «forzado» a autorizar la monitorización, luego en este segundo supuesto, el usuario paga una doble contraprestación: dinero y pérdida de privacidad[45].

Si esta es la situación, si los datos son la contraprestación o parte de la contraprestación, cabe preguntarse si es suficiente la ganancia que el consumidor recibe con el suministro del contenido digital. Se trata de un contrato, obviamente no gratuito, sino sinalagmático y, por ello, debe valorarse la justicia del intercambio que se realiza entre las partes, el equilibrio que el Derecho contractual debe asegurar en los negocios jurídicos privados. También cabe preguntase cuáles son los mecanismos que protegen al ciudadano ante una eventual utilización indebida de su información personal. La Directiva de contenidos digitales recoge las acciones que le asisten ante la falta de conformidad del bien o servicio digital adquirido, pero no protege otros derechos del usuario como sería, por ejemplo, en caso de resolución contractual, el derecho a que el proveedor no vuelva a utilizar sus datos personales. Ello se debe a que, realmente, no se concibe la información personal como un verdadero activo económico en manos del consumidor, como un elemento de intercambio entre el cliente

[45] Como muestra un botón: un consumidor que desea renovar la licencia anual del antivirus que tiene instalado en su PC. Recibe un correo electrónico-recordatorio recibido de la empresa para anunciarle que su licencia anterior está a punto de caducar (esto es, la empresa que ya recabó el correo electrónico del consumidor en el momento de la contratación de la licencia por primera vez, lo utiliza ahora para asegurarse la fidelización del cliente, recordándole en el momento oportuno que se le caduca la licencia y reconduciéndole a la fácil tarea de volver a pagar sin mirar lo que ofrecen y cobran los competidores en el mercado por el mismo servicio digital). Hasta aquí, podemos considerar que la compra de la licencia de antivirus y la aportación del propio correo electrónico fue un acto voluntario del consumidor y que, por tanto, la empresa está en su derecho de manejar esta información en su propio beneficio. Ahora bien, cuando el consumidor pulsa la tecla RENOVAR en el propio correo electrónico, se le abre una pantalla con la siguiente leyenda: *«Acerca de las cookies en este sitio. Este sitio web utiliza cookies propias y de terceros para mejorar tu experiencia de usuario y obtener información estadística. Para poder seguir navegando pulsa en «Sí, estoy de acuerdo». Podrás retirar este consentimiento en cualquier momento a través de las funciones de tu navegador. Ver nuestra política de cookies*». Estas advertencias unidas a una sola opción (pulsar la tecla SÍ, ESTOY DE ACUERDO), es todo lo que se le ofrece al consumidor. De este modo, su única decisión es la de renovar o no renovar el antivirus, y si decide hacerlo deberá necesariamente permitir tácitamente ser monitorizado, porque para renovar el antivirus hay que seguir navegando por la web y ello hace que la tecnología cookies se active automáticamente. Seguir navegando y pagar el precio del antivirus con la tarjeta, porque no es un servicio digital gratuito ¿Este consentimiento se parece en algo al que otorgó cuando optó por esta empresa para contratar la licencia?

y la empresa digital[46] y, por esta causa, se entiende que solo la normativa de protección de datos es la competente para velar por este derecho de la personalidad que es la privacidad de los ciudadanos. Veamos por qué los mecanismos que prevé el RGPD no son suficientes ni eficaces a estos efectos.

En primer lugar, son ineficientes, como ya se ha mencionado más arriba, porque las reclamaciones que en su caso interponga cada ciudadano ante la autoridad de control sólo servirán para solucionar su caso personal, no para evitar con carácter general el desequilibrio entre las prestaciones que se produce en las relaciones contractuales en el mercado digital, ni para cambiar el *modus operandi* de las grandes empresas digitales. En concreto, respecto al ejercicio del derecho de oposición, ya me he referido también a la dificultad que la propia tecnología representa para controlar el cumplimiento de lo dispuesto taxativamente en el art. 21.3 RGPD: *«Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines»*[47].

En cuanto a la reclamación que prevé el art. 82 RGPD, consiste en un régimen uniforme para toda Europa que reconoce a los titulares de datos personales una acción indemnizatoria contra los responsables y encargados del tratamiento, para resarcirse de daños y perjuicios sufridos a consecuencia de operaciones que estos lleven a cabo en infracción de lo previsto en

---

[46] Dice la Opinion 8/2016 del European Data Protection Supervisor, (7): *«En la UE, la información personal no puede concebirse como un mero activo económico: según la jurisprudencia del Tribunal Europeo de Derechos Humanos, el tratamiento de datos personales requiere protección para garantizar el disfrute del derecho a la vida privada y a la libertad de una persona de expresión y asociación. Además, el artículo 8 de la Carta de la UE y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) han consagrado específicamente el derecho a la protección de los datos personales. En consecuencia, el Reglamento general de protección de datos de 2016 contiene salvaguardas específicas que podrían ayudar a remediar los desequilibrios del mercado en el sector digital: las autoridades de protección de datos deben hacer cumplir la minimización de datos, que requiere que la información personal solo se procese donde sea adecuada, relevante y limitada a lo que es necesario en relación con los fines para los que se procesan', y el derecho de las personas a recibir información sobre la lógica involucrada en la toma de decisiones automatizada y la elaboración de perfiles»*. Consultable en https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en

[47] Al respecto, no obstante, hay que destacar el esfuerzo realizado por el legislador español para arbitrar mecanismos que hagan efectivo este mandato, y así el art. 15 de la Ley 3/2018 exige un comportamiento activo del responsable para impedir tratamientos futuros de los datos de quien ha ejercido el derecho de oposición. Por su parte, el art. 32 trata de concretar los sistemas para lograr el bloqueo de datos, si bien del redactado del artículo se desprende con claridad la dificultad técnica que encierran estos procesos, y la opción del legislador por dejar en manos de la Agencia Española de Protección de Datos y de las autoridades de control autonómicas, la decisión final de cómo proceder en cada caso.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

el Reglamento u otras normas relacionadas. Es claro que esta acción indemnizatoria es más detallada y precisa, y mejora el sistema previsto en la Directiva 95/46/CE, sin embargo, hay varias cuestiones que aún suscitan dudas, tal y como ya ha manifestado la doctrina[48], y que no ha resuelto para España la Ley 3/2018. El primer problema, a mi juicio, es que el art. 82 RGPD circunscribe la reclamación de indemnización al ámbito extracontractual, en España podría concebirse como una concreción de la norma general del art. 1902 del Código Civil español, que proviene de la aplicación directa de un Reglamento europeo. De hecho, la nueva ley española de protección de datos no contiene una disposición análoga al antiguo art. 19 de la Ley 15/1999. Por tanto, puede ocurrir, —y así lo han venido entendiendo los tribunales españoles— que el afectado acuda a la acción prevista en el art. 9.3 de la Ley Orgánica 1/1982 para la compensación de daños por intromisión ilegítima en los derechos al honor, a la intimidad y a la propia imagen, así como a la general de responsabilidad extracontractual del artículo 1902 CCE y, ahora, a la nueva acción establecida en el art. 82 RGPD. Pero ninguna de las tres constituye un remedio ante el incumplimiento contractual del responsable del tratamiento, cuando recibe la información personal del usuario a cambio del servicio digital contratado. En buena lógica, es necesario que el Derecho de contratos arbitre mecanismos de tutela en favor del contratante débil en el comercio electrónico, que no es otro que el ciudadano, el consumidor, de manera que pueda aplicar los pertinentes remedios de derecho contractual, también al aspecto de la privacidad. Los supuestos de antijuricidad del comportamiento (acción u omisión) contrario a las normas de protección de datos pueden ser muy diversos, la casuística es inmensa, pero está claro que muchos de ellos se producen en el contexto del contrato electrónico formalizado entre consumidores y prestadores de bienes o servicios. Por tanto, es necesario, en este ámbito como en tantos otros, delimitar hasta dónde llega la responsabilidad extracontractual y cuándo procede acudir a la responsabilidad contractual[49]. Ello, sin olvidar los

[48] Antonio Rubí Puig, «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», en *Revista de Derecho Civil* (2018), 53-87 (http://nreg.es/ojs/index.php/RDC). Ya había expuesto con gran claridad las quiebras del sistema con respecto a la acción civil del art. 19 de la antigua LOPD, Manuel Zunón Villalobos, en «La garantía civil de la privacidad», (BIB 2012\3488), *Revista Aranzadi Doctrinal*, 9, (2013), 1-23.

[49] Al respecto, la Sentencia del Tribunal de Justicia: asunto 189/87, Athanasios Kalfelis versus Banco Schröder, Münchmeyer, Hengst & Co., Banco Schröder, Münchmeyer, Hengst International SA y Ernst Markgraf, sentencia de 27 de septiembre 1988, párrafo 18 señalaba que la materia extracontractual, delictual o cuasidelictual, *«comprende toda demanda que se dirija a exigir la responsabilidad de un demandado y que no esté relacionada con la materia contractual»*. Por ello, si los datos personales son la contraprestación, obviamente constituyen materia contractual.

procedimientos administrativos ante la autoridad de control, que habitualmente vienen originados por los mismos comportamientos antijurídicos[50].

Por último, otra cuestión que está en el núcleo del desequilibrio entre las partes en la contratación electrónica, y ante la que se manifiesta la insuficiencia de la protección que ofrece la normativa sobre privacidad: la ausencia de una información clara e inteligible al interesado en el momento en que ha de decidir si entrega sus datos personales al empresario digital, y la articulación de sistemas engañosos de consentimiento tácito cuando lo hace. En efecto, la contratación electrónica se desarrolla a través de condiciones generales, de manera que la única opción de que dispone el interesado es la de adherirse al conjunto de cláusulas contractuales, o no hacerlo[51]. Me refiero una vez más a la autorización para el tratamiento de datos automatizado, y la creación de perfiles. Es cierto que el RGPD incluye la prohibición general de toda decisión basada únicamente en tratamientos de datos automatizados, pero también lo es que esta prohibición queda desactivada cuando es el propio interesado el que da su consentimiento[52], por ello es de capital importancia que se trate de un consentimiento informado y libre. Además, el comercio electrónico se desarrolla en gran medida por empresas no europeas, algunas de ellas —aunque no todas— sujetas al Escudo de la privacidad, que no prevé la necesidad del consentimiento del interesado en estos supuestos, luego puede ocurrir que los ciudadanos que contraten con estas compañías, aunque sean europeos, no

[50] La doctrina se pregunta por los problemas de coordinación entre el ejercicio de la acción indemnizatoria del artículo 82 RGPD y el seguimiento de un procedimiento administrativo sancionador por infracción de la normativa sobre protección de datos; así como los de coordinación entre el artículo 82 RGPD y otras acciones privadas de compensación de daños y perjuicios, ¿Sería posible acumular en una misma demanda para su tramitación en un único y mismo proceso, la pretensión indemnizatoria y las pretensiones de acceso, rectificación o supresión del RGPD? Por economía procesal, por evitar al perjudicado la carga de tener que iniciar varios procedimientos etc. pues estas acciones no solo no son incompatibles entre sí, sino que están todas ellas al servicio de la tutela de un mismo derecho, y derivan de unos mismos hechos. Pero, con respecto al sistema anterior al nuevo Reglamento Europeo y la nueva Ley de protección de datos, la doctrina jurisprudencial de la Audiencia Nacional y del propio Tribunal Supremo ha rechazado, sin excepción, cualquier intento de acumulación de la acción civil indemnizatoria, véase, por ejemplo, STS 28.12.2004 (RJ 2004, 8494); Antonio. Rubí Puig, «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 RGPD y otras acciones en derecho español», *Mimeo* (2018), 1-34.

[51] Klaus Jochen Albiez Dohrmann, «Las condiciones generales de la contratación: una lectura de los diferentes modelos de control», *Derecho contractual comparado. Una perspectiva europea y transnacional,* ed por Sixto Sánchez Lorenzo, (Cizur Menor, Civitas, 2013) 430-432.

[52] Art. 22.2 c) RGPD. Véase también Cdos. n.º 30, 38, 58, 60, 63, 68 y 70, así como a la regulación contenida en los arts. 13, 15, 21 especialmente.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

tengan garantía alguna ni opciones de impugnar el procesamiento de datos llevados a cabo sin intervención humana[53].

IV. La interacción (o la falta de ella) entre la normativa contractual y la de protección de datos

En este apartado me referiré al marco jurídico específico del comercio electrónico, para tratar de relacionarlo con lo expresado hasta aquí sobre la normativa de protección de datos. Ambas regulaciones confluyen y, por tanto, deberían interactuar para proteger al usuario persona física que interviene en la economía digital.

En el ámbito de la contratación electrónica nos encontramos tanto con los principios generales que afectan a las obligaciones y contratos, como con las normas específicas nacionales y supranacionales que afectan a los contratos electrónicos y, por supuesto, con toda la normativa especial aplicable en los casos en que uno de los contratantes tenga la condición de consumidor[54]. Tratando de seguir el mismo esquema que en el apartado anterior, trataré primero de identificar los principios rectores del comercio

---

[53] Por eso, el Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de sus datos (denominado habitualmente GT29), creado por la Directiva 95/46/CE, así como el Supervisor Europeo de Protección de Datos recomendaron en su día añadir una cláusula específica para el tratamiento automatizado de datos, por ejemplo, requiriendo la intervención humana o bien información adicional si así lo pedía el ciudadano europeo cuyos datos eran tratados. Sin embargo, la versión final del acuerdo no incorpora estos cambios. Cfr. EDPS Opinión 1/2016, p. 14.

[54] La normativa básica sobre el comercio electrónico que afecta a nuestro país se concreta hoy día a través de las Directivas europeas (Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, Directiva 93/13/CEE sobre cláusulas abusivas en contratos celebrados con consumidores, Directiva 1999/44/CE, de 25 de mayo, sobre determinados aspectos de la venta y las garantías de los bienes de consumo, Directiva 2011/83/UE sobre de derechos de los consumidores, así como laya referenciada Directiva 2019/770 de suministro de contenidos digitales. En cuanto a las leyes españolas aplicables: la Ley 31/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, la Ley 7/1998 de 13 de abril de Condiciones Generales de la contratación, el 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, entre otros.

Es de destacar que la reciente Ley 5/2019, de 15 de marzo, reguladora de los contratos de crédito Inmobiliario reforma el art. 5 de la Ley de condiciones generales que rezará del siguiente modo: *«5. La redacción de las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez. Las condiciones incorporadas de modo no transparente en los contratos en perjuicio de los consumidores serán nulas de pleno derecho»*. También añade un párrafo al art. 83 de la LGDCU, en el mismo sentido: *«las condicio-*

electrónico, y seguidamente me detendré en el consentimiento informado del consumidor, para concluirapuntando alguna idea sobre los remedios ante el desequilibrio contractual.

1. *Los principios que informan la contratación electrónica. La noción de desequilibrio contractual*

El Parlamentoeuropeo trabaja en estos momentos para sacar adelante la directiva sobre compraventa *on line* y *off line,* y ha promulgado ya la Directiva de suministro de contenidos digitales. Ello implicará una reforma de la Directiva europea de comercio electrónico, todo ello con la pretensión de dotar de mayor transparencia a las transacciones económicas desarrolladas en el contexto del comercio con consumidores, para que los usuarios tengan una mayor información, clara y comprensible, de quien es el responsable de la venta online en la que participan. Otro aspecto que afectará a la transparencia se regulará en relación a los servicios digitales gratuitos (aplicaciones gratuitas, redes sociales, etc.) puesto que el proveedor deberá poner a disposición de los usuarios una información previa a la contratación, así como ofrecerles de forma clara el derecho de desistimiento. Sin perjuicio de estas reformas, la regulación sobre comercio electrónico que data del año 2000, y todos sus desarrollos posteriores a nivel europeo y español, permiten extraer una serie de principios rectores de esta normativa contractual:

1. Principio de buena fe y de libertad contractual, como bases de todo el sistema. La regla de la buena fe procede de las codificaciones en materia civil y comercial, desde el siglo XIX y se extienden en el tiempo hasta nuestros días. En el ámbito del *soft law* europeo sobre derecho de contratos, los Principios Unidroit se refieren a la *good faith and fair dealing*, caracterizada como el buen comportamiento contractual. La lealtad contractual es objetiva, alude a la coherencia y al respeto del fin económico buscado. Finalmente, ha derivado en el moderno concepto de la razonabilidad. La necesidad de invocar un principio clásico como el de la buena fe nace del hecho de que el entorno en que se produce la contratación electrónica se presenta como desconocido, oscuro, menos fiable a priori que la contratación tradicional[55]. Y se complementa con el también clásico

nes incorporadas de modo no transparente en los contratos en perjuicio de los consumidores serán nulas de pleno derecho».

[55] Deepak Sirdeshmukh, Jagdip Singh, Barry Sabol, «Consumer Trust, Value, and Loyalty in Relational Exchanges», *Journal of Marketing,* (2002) 66-1, 15-37. Consultable en https://doi.org/10.1509/jmkg.66.1.15.18449

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

principio de libertad contractual, que se aplica del mismo modo en la contratación electrónica y en la tradicional, y cuyos límites nunca vendrán impuestos por el uso de la tecnología, sino por el hecho de contratar con consumidores[56].

2. Principio de seguridad jurídica, especialmente en el proceso de formación de los contratos electrónicos. Esta seguridad jurídica se presupone cuando la contratación electrónica se desarrolla a través del intercambio electrónico de datos (EDI, en sus siglas en inglés), pues los operadores económicos tienen que concluir un acuerdo previo de intercambio electrónico de datos, que suele ajustarse al modelo elaborado por algún organismo internacional[57]. En cambio, cuando la contratación electrónica se lleva a cabo a través de una red abierta como Internet la seguridad jurídica es mucho más dudosa. De ahí, la búsqueda de la seguridad jurídica a través de los textos internacionales de armonización[58].

3. Principio de equivalencia funcional, que implica que una transacción efectuada en papel y otra efectuada a través de medios electrónicos deban recibir el mismo tratamiento legal. El principio de equivalencia funcional no presupone la efectividad legal del medio electrónico empleado, ya que éste estará sujeto a los mismos requisitos de prueba que cualquier otro. Lo que implica es que el medio empleado para realizar la transacción es irrelevante[59]. La equivalencia funcional se vincula directamente con el principio de neutralidad tecnológica de las normas, que impone al legislador la obligación de definir los objetivos a conseguir, sin imponer ni discriminar el

---

[56] Rodolfo Fernández, *Contratación electrónica: la prestación del consentimiento en Internet*, (Barcelona, Bosch, 2001).

[57] Como el Modelo Europeo de Acuerdo elaborado bajo los auspicios de la Comisión Europea, (véase DOCE 1994 C 338/100).

[58] Ya he mencionado los Principios Unidroit, PICC. También han procurado establecer unas pautas uniformes para la contratación en Europa los Principios de Derecho contractual europeo, PECL, el borrador académico del Marco Común de Referencia, DCFR, la Normativa Común de Compraventa europea, CESL, entre otros. Véase Jose Antonio Castillo Parrilla «El impulso normativo europeo en el marco de la estrategia para el mercado único digital de Europa y los principios de la contratación electrónica en España. Especial referencia al contrato para el suministro de contenidos digitales», *Contratación electrónica y protección de los consumidores op. cit.*, 116.

[59] Pero el alcance de este principio puede ser limitado, puesto que en algunas normas no se reconoce de manera incondicional, sino que se hace depender del acuerdo previo sobre el empleo de medios electrónicos. Rosa Julia Barceló, *Comercio electrónico entre empresarios. La formación y prueba del contrato electrónico*, (Valencia, Tirant lo Blanch, 2000), 169; Pilar Jiménez Blanco, «Contenido y condicionantes de las obligaciones contractuales» *Derecho Contractual comparado, una perspectiva europea y transnacional*, ed. por Sixto Sánchez Lorenzo, I, (Pamplona, Aranzadi, 2016), 881.

uso de cualquier tipo de tecnología para conseguirlos[60]. De manera que deberá elaborar reglas neutrales, es decir, que no estén asociadas con un tipo determinado de tecnología[61]. Por último, el art. 80 de la nueva Ley 3/2018 de protección de datos española proclama el derecho a la neutralidad de Internet. Se reconoce a los usuarios un derecho cuyo contenido se concreta en la obligación de los proveedores de servicios de Internet de proporcionar *«una oferta transparente de servicios sin discriminación por motivos técnicos o económicos»*.

A mi juicio, estos principios no se están respetando en la actualidad en el contexto del comercio electrónico con consumidores, y en lo que respecta al trasvase de información personal. En la actualidad es prácticamente imposible saber cuándo estamos siendo monitorizados y qué usos posteriores se le va a dar a nuestra información más personal. No puede negarse la situación de desequilibrio contractual del usuario titular de su propia privacidad.

En efecto, los contratos digitales son siempre de adhesión[62], articulados mediante condiciones generales y, en concreto las cláusulas que se refieren a la materia de la privacidad son larguísimas y complejas condiciones generales que se presentan al usuario bajo la rúbrica *«políticas de privacidad»*. Los términos sobre protección de datos aparecen ocultos en conjuntos complejos de cláusulas estándar. Los consumidores tienden 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 que se presentan como rápidos, cómodos e, incluso, en ocasiones, *gratuitos*[63]. Así pues, el desequilibrio contractual se deriva de la ventaja injusta que favorece al proveedor digital frente a la debilidad del usuario. El proveedor es la parte fuerte en la relación contractual puesto que proporciona sus servicios por un precio

---

[60] Cristina Culell March, «El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico» *IDP: revista de Internet, derecho y política,* 11 (2010*)* 3.

[61] No obstante, también hay detractores de este principio los cuales entienden que, al no prever las normas ninguna tecnología ni exigir unos estándares para las firmas electrónicas, pueden resultar un tanto ambiguas. Véase Marina C. Silveira, «Repercusiones internacionales del comercio electrónico: el marco legal del comercio electrónico en América latina y la necesidad de armonizar la normativa aplicable», *Revista de Contratación electrónica*, 18, (2001), 6.

[62] Sobre el contrato electrónico véase, Pedro Grimalt Servera, «La formación del contrato celebrado por medios electrónicos» en *Negociación y perfección de los contratos,* ed. por M.ª Angeles Parra Lucan, (Cizur Menor, Aranzadi, 2014), 355 y ss.

[63] Bart W. Schermer Bart Custers, Simone van der Hof', «The Crisis of Consent: how Stronger Legal Protection may Lead to Weaker Consent in Data Protection» 16. *Ethics and Information Technology* (2014) 171-182.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

muy superior a su verdadero valor: la autorización para arrebatar al usuario su privacidad —para sí y para terceros—, y realizar después un tratamiento automatizado de dicha información personal, que redunda exclusivamente en su propio beneficio.

En conclusión, no hay equivalencia funcional ni neutralidad de internet: basta constatar los avances logrados en defensa de los consumidores en el sector de la contratación bancaria, que sin embargo no se aprecian en el comercio electrónico con respecto a las cláusulas sobre privacidad de los usuarios. Los contratos bancarios también son de adhesión, se redactan en papel —la mayoría de las veces en documento público—, y hoy día ya no pueden contener cláusulas generales redactadas de forma no transparente, puesto que han sido expulsadas del contrato, calificadas como nulas de pleno derecho[64]. Esto no ocurre en el comercio realizado por internet. Los intereses de marketing y de control del mercado de las grandes empresas digitales prevalecen sobre su obligación de transparencia cuando formalizan negocios jurídicos con consumidores.

2. *El consentimiento del usuario para la cesión y posterior tratamiento de sus datos personales*

El consentimiento del titular de los datos es uno de los pilares en el que se fundamenta la protección de datos. Según el RGPD, la cesión de los datos para su tratamiento siempre debe ser inequívocamente consentida sobre la base de un conocimiento cabal y previo a la cesión. También el consentimiento constituye la manifestación por excelencia de la libertad contractual. Sin consentimiento no puede haber contrato. Sin embargo, los mecanismos implementados en la economía digital para informar al consumidor y para recabar su consentimiento pueden constituir en ocasiones un límite en el ejercicio de su autonomía privada, por parte del consumidor. Es necesario evaluar, con respecto a la transmisión de la propia privacidad, los instrumentos de Derecho contractual tradicionalmente relacionados con situaciones exclusivamente patrimoniales. La presencia de un contrato bilateral de adhesión entre el proveedor electrónico y el consumidor hace necesaria una revisión de las condiciones generales del contrato. Se trata de asegurar que el usuario autoriza libremente todas las cuestiones relativas a su privacidad.

Según el artículo 4.11 RGPD, se entiende por consentimiento del afectado *toda manifestación de voluntad libre, específica, informada e inequí-*

[64] Véase nota 54.

voca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. 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, es decir, debe solicitarse y recolectarse la información personal de forma individualizada, no en masa, obteniendo un consentimiento diferenciado para cada finalidad diferenciada del tratamiento de los datos recabados. Por tanto, una sola casilla general de aceptación de la política de privacidad, que además aparece ya premarcada en una página web, no tiene validez como consentimiento[65]. La solicitud de su consentimiento al usuario ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el cual se está solicitando.

Sin embargo, es habitual ver en las webs mensajes requiriendo el consentimiento para el uso de cookies, que perturban *de facto* el acceso al servicio o a la información, de modo que el usuario clica en ACEPTO, para poder seguir navegando. El consentimiento para la cesión de la propia privacidad constituye, así, una condición para poder acceder al servicio «gratuito» de internet. Por ello, precisamente, se suceden los permisos «inconscientes» de los usuarios. Se trata de una práctica engañosa empleada por el empresario digital para recabar la información personal de los usuarios en grandes dosis, todo lo cual coloca al consumidor en una posición de debilidad frente a la otra parte contratante.

El art. 7.4 RGDP establece que no puede supeditarse la ejecución de un contrato, es decir, la entrega del bien o la prestación del servicio contratado, a que el afectado consienta el tratamiento de datos *no necesarios* para la ejecución del contrato. Luego, el legislador europeo cuenta con que la empresa pretenda obtener más información privada que la que realmente necesita para el desarrollo de su actividad negocial, y le permite solicitarla, siempre que el usuario consienta en esta entrega de su privacidad, y que tal entrega no condicione el cumplimiento contractual del proveedor. Por su parte, el art. 6.3 de la ley española de protección de datos impide supeditar la ejecución del contrato al hecho de que el usuario autorice el tratamiento de sus datos *para finalidades diferentes,* que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual. Por tanto, en ambos supuestos el legislador contempla

[65] El art. 7.2 RGPD insiste en la necesidad de separar entre les diferentes disposiciones contractuales, la relativa al tratamiento de los datos personales del cliente y, dentro de esta, las diversas finalidades de este tratamiento. El objetivo de la norma es que el sujeto pueda conocer y entender, claramente, los permisos que se le están solicitando de modo que pueda en su caso, consentir una cláusula y rechazar otra.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

y permite la posibilidad de que no se cumpla con el principio de minimización de datos. No puede decirse que el derecho fundamental al control de la propia privacidad, del que somos titulares las personas físicas, quede especialmente salvaguardado con la normativa vigente de protección de datos.

2.1. El consentimiento debe ser informado: deberes de información precontractual del empresario

El consentimiento para el tratamiento de la información personal debe ir precedido de una información suficiente al respecto. El RGPD consagra el principio de transparencia[66], estableciendo una lista exhaustiva de la información que debe proporcionarse a los interesados, más amplia que la que contenía la norma anterior[67]: la existencia del fichero o tratamiento, su finalidad y destinatarios; el carácter obligatorio o no de la respuesta, así como sus consecuencias; la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; la identidad y datos de contacto del responsable del tratamiento, los datos de contacto del Delegado de Protección de Datos, en su caso etc., incluso la intención del responsable de transferirlos a otros sujetos, si fuera el caso. La información a los interesados deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Así, el RGPD prevé que la información precontractual pueda proporcionarse en combinación con iconos estandarizados que ofrezcan una visión de conjunto del tratamiento previsto[68].

Esta normativa exigente sobre la información precontractual se acerca mucho a la que persigue la transparencia de las condiciones generales no negociadas, que se imponen por una de las partes contratantes en los contratos con consumidores[69]. Estos deben ser capaces de comprender la utilización que de sus datos personales va a hacerse, de modo que

---

[66] Cdo. 58 RGPD.

[67] Arts. 13 y 14 RGPD.

[68] Cdo. 60 RGPD: *«(…) Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente».*

[69] «La LSSICE no prevé ninguna sanción civil por el incumplimiento del deber precontractual de informar; sin embargo, el no informar correctamente al destinatario, puede tener sus consecuencias desde la perspectiva de la validez del contrato, siempre que esa falta de información haya podido inducir a error (vicio) en el afectado en el momento de prestar su consentimiento» Pedro Grimalt «La formación del contrato celebrado por medios electrónicos» *op. cit*,,371.

puedan otorgar un consentimiento válido para el tratamiento de éstos y, en ningún caso, los costes de ejercer sus derechos fundamentales pueden exceder a los beneficios de hacerlo. Pero la realidad de las webs comerciales, y de la información sobre las políticas de privacidad de las empresas digitales es bien diferente. No suelen ofrecerse servicios fáciles de usar y respetuosos con la privacidad. Y ello es así porque resulta incompatible con las actuales prácticas de negocio, que usan los datos personales y explotan su valor económico sirviéndose, para ello, de cláusulas informativas opacas o engañosas. Sin embargo, deben calificarse como verdaderas condiciones generales y, por ello, sujetas a la Directiva 93/13/CE sobre cláusulas abusivas en contratos celebrados con consumidores: son cláusulas contractuales que se han redactado previamente sobre las que el consumidor no ha podido influir en modo alguno, y a las que se limita a adherirse.

Para determinar la arbitrariedad de una condición general de la contratación, la Directiva 93/13 prevé dos tipos de controles: un control de incorporación —si la cláusula contractual estaba redactada de forma entendible para el consumidor— y un control de contenido —si dicha cláusula crea un desequilibrio entre los derechos y obligaciones de las partes que se derivan del contrato—[70]. Por tanto, señala el legislador europeo[71], las condiciones generales serán abusivas cuando pese a las exigencias de la buena fe, causen un desequilibrio importante ente los derechos y obligaciones de las partes que se derivan del contrato, en detrimento del consumidor.

Así, pues, y siguiendo con el ejemplo expuesto más arriba, una web que solo presenta la casilla *«He leído y acepto la política de privacidad»* como fórmula global para recoger en bloque todos los consentimientos del usuario, aunque se pueda acceder a la referenciada política de privacidad de la empresa si el usuario se molesta en clicar en el link correspondiente, no es una fórmula correcta, porque no facilita la comprensión de la autorización que el usuario está llevando a cabo ni la realización de un acto afirmativo, reflejo de una voluntad libre ex art. 4.11 RGPD. Al contrario, lo que facilita es que el usuario acepte la cesión sin haber leído los términos del contrato[72]. En-

[70] Mireia Artigot Golobardes, «Una mirada desde la economía digital de la regulación de la compraventa en el Libro VI del Código Civil de Cataluña» *Estudios sobre el Libro VI del Código civil de Cataluña*, ed. por Angel Serrano de Nicolas (Barcelona, Marcial Pons, 2018), 53.

[71] Art. 3 Directiva 93 /13/CE.

[72] Como muestra un botón: la cláusula que es necesario clicar para poder comprar un billete de tren a través de la web Renfe.com: *«He leído y acepto Condiciones Generales de Viajeros, las Condiciones Generales de la venta y la Política y Privacidad disponibles en la Información Legal.»*.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

tiendo que esta cláusula se puede calificar de abusiva por no superar el control de incorporación de forma suficientemente transparente para el consumidor. Y si es abusiva, es nula de pleno derecho ex art. 5 de la Ley de condiciones generales de la contratación, en su última versión recientemente reformada.

Desde una perspectiva del análisis económico del derecho, el contrato de adhesión relativo a la cesión de la privacidad del usuario solo será completo si se articula mediante un formulario en línea de solicitud de datos adaptado a cada necesidad, dirigido a solicitar realmente solo los datos necesarios. Y en el que se soliciten los permisos suficientes y se proporcione la información precontractual necesaria para que el usuario pueda decidir qué datos proporciona y cuáles no. O para informarle de los datos que no son necesarios y que aun así se solicitan, para que pueda decidir si los presta o no y, de esta manera, sea consciente de que está pagando una contraprestación por el servicio digital, en forma de datos. En el bien entendido de que, si se condiciona la prestación de un servicio digital a la proporción de esos datos no necesarios, se produce inmediatamente un desequilibrio contractual, máxime teniendo en cuenta que esa información a la que se condiciona el servicio proporciona al proveedor una altísima rentabilidad económica, muy superior al valor económico que cabe atribuir al bien o servicio que recibirá el usuario-consumidor.

La pregunta que cabe formularse es cómo va a repercutir, o mejor, si va a repercutir de algún modo en la contratación electrónica y, más en concreto, en la negociación sobre la propia privacidad, la batalla librada por la doctrina y, muy especialmente, por los tribunales para hacer cada vez más informado y consciente el consentimiento del consumidor respecto de las cláusulas predeterminadas incluidas en las condiciones generales de los contratos. La lucha librada durante las últimas épocas por aflorar las cláusulas abusivas y lograr su supresión de los contratos en los que existe una clara asimetría entre las partes. En definitiva, qué papel juega el moderno derecho de consumo en el ámbito de la protección de los datos personales.

2.2. El consentimiento se puede revocar: el control del usuario sobre los permisos concedidos para el tratamiento de su privacidad

Afirma nuestro Tribunal Constitucional que el derecho a la protección de datos consiste en la potestad de control del individuo sobre sus propios datos personales[73]. De esta definición se infiere que el ciudadano puede

[73] Véase nota 25 sobre la STC 292/2000.

ejercer en cualquier momento el derecho de oposición al tratamiento que se está haciendo de su información personal, solicitando la supresión de los datos o la limitación del tratamiento. Todo ello está conectado también con el derecho al olvido, una conquista reciente también exigible al proveedor de bienes y servicios en la contratación electrónica, y que es fruto, sobre todo, de la labor de los tribunales[74]. Establece el art. 7.3 RGPD: *«El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo»*[75].

La dicción literal de la norma es taxativa, sin embargo, surgen diversos interrogantes acerca de su eficacia práctica. Por ejemplo, en el contrato de suministro de contenidos digitales a cambio de información personal, ¿qué consecuencias tendría esta retirada del consentimiento por parte del consumidor para la utilización de sus datos, si estos eran la contraprestación por el servicio digital? ¿puede identificarse con un incumplimiento contractual por parte del usuario? ¿y si el proveedor ya se ha servido de esta información y ha realizado el tratamiento previsto (técnicas de elaboración de perfiles, estudios comportamentales o reventa de datos a terceros) ¿se podría entender que el usuario ha pagado el precio del servicio y, por tanto, debe poder seguir accediendo al contenido digital aunque haya retirado su consentimiento? De hecho, la Directiva no especifica la naturaleza del contrato de suministro de contenidos digitales a cambio de privacidad[76]. Se trata de un contrato oneroso, eso es claro, pero

---

[74] A este respecto constituye un hito y un referente la sentencia del Tribunal de Justicia de la Unión Europea en el Asunto C-131/12, Google Spain SL versus la Agencia Española de Protección de Datos, de 13 de mayo de 2014 (ECLI: EU: C 2014: 85). Veáse también Serafina Larocca,«Revocación del consentimiento contractual para el tratamiento de datos y el derecho al olvido», *Contratación electrónica y protección de los consumidores op. cit*., 65-74

[75] El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de sus datos (GT29) establece que *«(…) la inclusión de disposiciones y considerandos específicos sobre la retirada del consentimiento confirma que el consentimiento debe ser una decisión reversible y que el interesado sigue manteniendo un cierto grado de control»,* «Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, 17/ES.

[76] «*La propuesta evita deliberadamente diferenciar entre distintos tipos de acuerdos contractuales, v. gr., contratos de compraventa o de servicios, para evitar que la nueva Directiva quede desfasada por el rápido desarrollo tecnológico y el alto nivel de innovación y evolución de los nuevos modelos de negocio en el mercado digital»,* Gerald Spindler, «Contratos de suministro de contenidos digitales: ámbito de aplicación y visión general de la Propuesta de Directiva de 9.12.2015», *InDret* 3 (2016) 6; véase también Reiner Schulze, «Nuevos retos para el Derecho de contratos europeo y cuestiones específicas acerca de la regulación del suministro de contenidos digitales», *La europeización del derecho*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

no contiene una obligación de dar. Porque los datos personales —en tanto que derechos de la personalidad— no se dan para siempre, se cede su explotación sólo temporalmente, y con posibilidad de revocación en todo momento.

Se puede poner en relación esta facultad del usuario para decidir sobre el consentimiento prestado en relación con su privacidad, con la facultad de desistimiento del contrato que asiste al consumidor, que le permite desistir sin causa alguna, siempre que se observen determinados requisitos[77]. El derecho de consumo prevé la obligación del empresario de informar cumplidamente sobre la forma y el plazo y los procedimientos del desistimiento contractual. La falta de información previa sobre este punto vulnera, obviamente, la norma europea sobre cláusulas abusivas y sobre derechos de los consumidores, tal y como ha recordado el TJUE en una reciente sentencia que tiene la virtualidad de referirse a un contrato de compraventa celebrado a distancia[78], esto es, como los contratos que se celebran en el mercado digital: «*cuando el contrato se celebre mediante una técnica de comunicación a distancia en la que el espacio o el tiempo para facilitar información sean limitados, el comerciante está obligado a dar a conocer al consumidor, a través de la técnica en cuestión y antes de la celebración del contrato, las condiciones, el plazo y los procedimientos para ejercer ese derecho. En tal caso, ese comerciante debe facilitar al consumidor el modelo de formulario de desistimiento*» [79]. Trasladando analógicamente esta doctrina al ámbito de los datos personales, y de conformidad con el art. 7.3 RGPD debería ser relativamente sencillo revocar el propio consentimiento para el uso de nuestra información personal, el empresario digital debe facilitarlo y no obstaculizarlo. Pero lo cierto es que las grandes compañías no van a renunciar al análisis de datos y a los

---

privado: cuestiones actuales, ed. por Esther Arroyo Amayuelas y Angel Serrano de Nicolas, (Barcelona, Marcial Pons, 2016), 17.

[77] Manuel Jesus Marín López, «La formación del contrato con consumidores», *Negociación y perfección de los contratos, op. cit.*, 839-841.

[78] Art. 92.1 TRLGDCU, que define lo que puede entenderse por contrato celebrado a distancia, e incluye de forma explícita la contratación en línea. Luis María Miranda Serrano, «Contratos celebrados a distancia. Comentario de los arts. 92 a 106 TRLGDCU», *La defensa de los consumidores y usuarios. Comentario sistemático del texto refundido aprobado por el real decreto legislativo 1/2007* ed. por Manuel Rebollo Puig y Manuel Izquierdo Carrasco, (Madrid, Iustel, 2011), 1443-1562.

[79] La STJUE es la dictada en el Asunto C-430/17, Walbusch Walter Busch GmbH & Co. KG versus Zentrale zur Bekämpfung, Sentencia de 23 de enero de 2019. Véase también Christian Twigg-Flesner, «La Directiva sobre derechos de los consumidores en el contexto del Derecho de consumo de la Unión Europea», *La revisión de las normas europeas y nacionales de protección de los consumidores*, ed. por Sergio Cámara Lapuente, (Cizur Menor, Civitas, 2012), 97.

estudios de mercado[80], y hasta cierto punto se puede decir que la norma europea les ampara, puesto que incluye dentro del concepto de «intereses legítimos», los objetivos de marketing y mercadotecnia directa[81]. No debe uno llamarse a engaño, es el legislador quien no otorga al consentimiento del usuario para la cesión de la propia privacidad la relevancia jurídica que cabría esperar. En la contraposición de los intereses en juego, es más importante el valioso activo que para las empresas constituye la información personal de sus usuarios, que el ejercicio por parte de estos de su derecho a controlar su propia información personal[82].

V. **Reflexiones finales**

En las líneas precedentes he tratado de dibujar los trazos esenciales del contrato de adhesión para la cesión de datos personales, que los usuarios formalizan en el contexto de la contratación electrónica en el ámbito privado. Las cláusulas contractuales son, en definitiva, el vehículo en el que transitan los derechos y libertades de las personas físicas. En cuanto al derecho a proteger la propia privacidad, los estándares europeos de protección son, en princi-

---

[80] Reproduzco el contenido de un e-mail recibido de la empresa Booking.com, ante la petición de un usuario que expresa su voluntad de revocar el consentimiento para el tratamiento de sus datos: *«Entendemos por tu e-mail que no quieres que compartamos tus datos personales con otras marcas del grupo Booking Holdings. Con este mensaje queremos confirmar que no compartiremos tus datos para personalizar tu experiencia cuando utilices los servicios de las otras marcas del grupo. Sin embargo, no podemos dejar de compartir tus datos personales con las otras marcas de Booking Holdings en los casos en los que sea necesario hacerlo para cumplir con nuestras obligaciones legales y para: 1) Poder ofrecerte los servicios que has solicitado, así como servicios de atención al cliente. (…) 2) Detectar, prevenir e investigar actividades fraudulentas e ilegales. Creemos que tenemos motivos legítimos para compartir tus datos personales con otras marcas del grupo Booking Holdings con el objetivo de detectar, prevenir e investigar actividades fraudulentas (…) 3) Mejorar los análisis de datos y el producto. Creemos tener motivos legítimos para compartir tus datos personales con otras marcas del grupo Booking Holdings para desarrollar el análisis de datos con el objetivo de mejorar nuestros productos y servicios. El objetivo principal es optimizar y personalizar tanto nuestra plataforma online como la de otras marcas del grupo Booking Holdings para que se ajuste más a tus necesidades y sea más fácil de usar. Nuestro objetivo es tomar las medidas tecnológicas necesarias, como el enmascaramiento de datos, para usar información pseudoanónima para mejorar el análisis de datos y el producto. Esto significa que no usaremos tu nombre, dirección de e-mail, dirección postal ni número de teléfono, sino que reemplazaremos esos datos con un número identificativo único. En los casos de estos 3 supuestos específicos, creemos que nuestros intereses legítimos se anteponen a las libertades y los derechos de privacidad».*

[81] Me he referido a este aspecto en el apartado anterior del trabajo, con cita del Cdo. 47 del Reglamento.

[82] Caggiano, «A quest for efficacy…», *op. cit.*,15.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

pio, razonablemente elevados y, además, Europa trata de extender un umbral de seguridad en relación con la circulación de los datos personales y la protección de la privacidad, incluso fuera de sus propias fronteras. No obstante, no puede decirse que lo haya conseguido, porque ha pesado más el interés económico de las grandes compañías que operan en internet y se nutren de grandes dosis de información personal de los usuarios. En efecto, la Carta de los Derechos Fundamentales de la UE configura el consentimiento solo como uno de los fundamentos para legitimar el tratamiento de datos personales. El RGPD prevé un sistema en el que la necesidad del consentimiento podría ser interpretada restrictivamente o, incluso, que tal necesidad del consentimiento del usuario pudiera obviarse en determinados casos.

A pesar de todo, entiendo que el hecho de que el procesamiento de datos personales pueda fundarse en bases legítimas distintas del consentimiento no excluye, o no debería excluir, el equilibrio necesario de estos otros intereses con las libertades fundamentales de los ciudadanos. En la emisión del consentimiento para la cesión de los propios datos deben concurrir los principios básicos de la contratación con consumidores: el respeto a la autonomía de la voluntad del consumidor, la información completa y clara, previa al ejercicio de dicha libertad contractual. Se trata de promover la aplicación de la llamada *privacy by design*, que impide a las compañías presuponer el consentimiento tácito por el hecho de navegar por ciertas redes, o utilizar determinados servicios de Internet. Que el consentimiento sea explícito, cuando se trata de autorizar la monitorización de las actividades del usuario en la red, así como el almacenamiento y tratamiento de sus datos personales. Ahora viene ocurriendo justo todo lo contrario. Es importante también abordar una tarea de educación de la ciudadanía, enseñar a los consumidores el valor de su privacidad para que la defiendan, lo mismo que han hecho anteriormente con su dinero, planteando y ganando importantes batallas en el sector de la contratación financiera.

Por último, debo insistir en que queda mucha tarea por hacer. Debería seguir explorándose sobre los remedios que asisten al usuario-consumidor ante una situación de desequilibrio, que resulta palmaria. ¿Cabe plantearse alguno de los remedios de la moderna doctrina desarrollada en los textos internacionales de armonización, sobre la ventaja injusta y la protección al contratante más débil?[83] ¿Son más eficientes las soluciones que propone el Derecho de consumo a las que me he referido sucintamente en el texto? En cualquier caso, el Derecho contractual puede y debe interactuar con el régimen jurídico de la protección de datos, para tratar de proteger el ejercicio por las personas físicas de su derecho a proteger y defender su propia privacidad.

[83] Esther Gómez Calle *Desequilibrio contractual op. cit.*, 96 y ss.

Sobre la autora

La doctora **Paloma de Barrón Arniches** es profesora agregada de la Facultad de Derecho de la Universidad de Lleida, adscrita al Departamento de Derecho Privado. Sus principales ámbitos de interés son en primer lugar, el derecho de sucesiones, materia a la que ha dedicado una monografía, El pacto de renuncia a la legítima futura (ISBN: 8495665107), así como numerosas publicaciones en revistas y libros colectivos (Ej. Libertad de testar y desheredación en los derechos civiles españoles, InDret, octubre 2016, http://www.indret.com/pdf/1258_es.pdf). En segundo lugar, cabe destacar su interés por el derecho de obligaciones y contratos desde la perspectiva del proceso de armonización del derecho privado en la Unión Europea, y su influencia en el desarrollo y modernización del derecho de obligaciones español. Al respecto cabe destacar la monografía: El contrato de servicios en el nuevo Derecho contractual europeo (ISBN:978-84-290-1680-2), así como otras publicaciones que se desarrollaron en el marco de sendos proyectos de investigación financiados por el MICINN, como el titulado «El proyecto de marco común de referencia: comentario académico desde el derecho contractual español». En la actualidad, el análisis de la materia contractual por parte de la autora se ha centrado en el comercio electrónico y todos los negocios jurídicos que se realizan on line, básicamente desde la perspectiva del consumidor y en relación con su derecho a la protección de los propios datos personales.

About the Author

Ms. **Paloma de Barrón Arniches** is an associate professor at University of Lleida, attached to the Department of Private Law. Her main areas of interest are, first of all, inheritance law, a subject to which she has dedicated a monograph, El pacto de renuncia a la legítima futura (ISBN: 8495665107), as well as numerous publications in Journals and collective books (Eg: Libertad de testar y desheredación en los derechos civiles españoles, InDret, October 2016, http://www.indret.com/pdf/1258_es.pdf). Secondly, she is interested in contract law from the perspective of the process of harmonization of private law in the European Union, and its influence in the development of the Spanish law of obligations. In this respect, the monograph El contrato de servicios en el nuevo Derecho contractual europeo (ISBN:978-84-290-1680-2) should be noted, as well as other publications which were developed in the context of both projects, financed by the MICINN, (Eg.:«El proyecto de marco común de

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 61/2019, Bilbao, págs. 29-65
doi: http://dx.doi.org/10.18543/ced-61-2019pp29-65 • http://ced.revistas.deusto.es

referencia: comentario académico desde el derecho contractual español»). Currently, the author's analysis of the contractual subject is focused on electronic commerce and all the on-line contracts, from the perspective of the consumer and their right to the protection of personal data.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. 61/2019, Bilbao

Derechos de autor

Copyright