InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?

Luz M. Martínez Velencoso
Marina Sancho López

Facultad de Derecho
Universitat de València

BARCELONA, ENERO 2018

Abstract[*]

Los avances en tecnología precisan de nuevas respuestas por parte del legislador en todos los sectores. Así, en el ámbito de la contratación, la Unión europea ha puesto en marcha la Agenda Digital, entre cuyos objetivos se encuentra ayudar a los agentes económicos a aprovechar todo el potencial que tienen las TIC. En este contexto se encuadran las Propuestas de Directiva sobre compraventa on-line y sobre suministro de contenidos digitales, que tienen como finalidad última promover el mercado digital. En este proceso de implementación normativa es importante valorar los riesgos que las nuevas tecnologías llevan implícitos, como la necesidad que tienen los consumidores de revelar datos como condición para el suministro de "bienes digitales". El "mercado de datos" es un negocio suculento en Internet, donde muchas empresas que negocian con datos están obteniendo enormes beneficios, con el peligro que ello supone para la privacidad de los ciudadanos. La Propuesta de Directiva sobre contenidos digitales pretende mejorar la protección de los derechos de los ciudadanos en este ámbito, sin renunciar al objetivo de fomentar el mercado digital. De este modo, se prevé como contraprestación por los contenidos digitales la entrega de datos personales. El problema es que esta categoría no encaja bien dentro de la dogmática jurídica tradicional, porque los datos personales, protegidos en cuanto que manifestación de la personalidad, no pueden ser entendidos en sí mismos como "commodity" (aunque puede admitirse, en algunos casos, la validez del negocio jurídico en cuya virtud el sujeto capaz haga una cesión de alguno de estos derechos a cambio de una contraprestación). En cualquier caso, el desarrollo legislativo de esta cuestión debería estar en consonancia con la normativa europea sobre protección de datos personales.

Advances in technology require new responses from legislator in all areas. Thus, in the field of contract law, the European Union has launched the Digital Agenda, among whose goals is to help economic agents to take advantage of the potential of ICTS. Inside this context are the proposed online sale of goods Directive and a second proposal for a directive on the supply of digital content, both oriented to promote the digital market. In this process of implementing legislation, it is important to assess the risks implicit in the new technologies, such as the need for consumers to disclose data as a condition for the supply of "digital goods". The "market data" is a succulent business on the Internet, where many companies that negotiate with data are obtaining enormous profits, with the danger that this entails for the privacy of citizens. The proposal for a directive on digital content aims to improve the protection of the rights of citizens in this area, without renouncing the objective of promoting the digital market. Consequently, it is regulated as compensation for the digital content, the delivery of personal data. The problem is that this category does not fit well within the traditional legal dogmatic, because the personal data, protected as a manifestation of the personality, cannot be understood as "commodity" (other question is the possible commercial exploitation under certain circumstances). In any case, the legislative development of this issue should be in line with the European rules on protection of personal data.

Title: The new concept of onerousness in the digital market. Is it really free the App?

Palabras clave: Derecho y nuevas tecnologías, onerosidad, contrato de suministro de contenidos digitales, datos como contraprestación, transparencia, privacidad, Big data, data brokers, Facebook

[*] Marina Sancho López es investigadora contratada por el Proyecto Prometeo II, 2015-14 "Derecho Civil Valenciano y Europeo", Universitat de València. Es autora de los epígrafes 2-5 (ambos inclusive) de este trabajo.

Keywords: Law & New technologies, onerousness, supply of digital content contract, data as counter performance, transparency, privacy, Big data, data Brokers, Facebook

Sumario

1. El Derecho ante la Revolución digital

1.1. Introducción

La tecnología avanza muy rápidamente, como somos capaces de observar. No sucede lo mismo con el Derecho, que muchas veces reacciona cuando ya se han planteado los problemas y éstos deben ser resueltos. En este sentido, el legislador se enfrenta al problema de la revolución digital, en sus varias facetas. Una de ellas tiene que ver con el Derecho de los contratos, teniendo en cuenta que cada vez es más frecuente concluir contratos a través de Internet, y no siempre contratos de compraventa, sino también contratos de prestación de servicios, de suministro de contenidos digitales…A veces sucede, dada la particularidad de esta forma de contratar, que las categorías clásicas del Derecho contractual no siempre encajan bien.

En el ámbito de la Unión europea, esta forma de contratación fue objeto de regulación por la propuesta de Reglamento de Compraventa europea, que como es sabido, finalmente fue abandonado, pese a las grandes expectativas que el mismo suscitó sobre todo a nivel académico, como lo demuestran la cantidad de comentarios que fueron publicados en distintas lenguas y países.
Una única regulación del contrato de compraventa en Europa se decía que tendría grandes ventajas y fomentaría la contratación al eliminarse los costes de transacción que venían representados por la existencia de distintas regulaciones a nivel nacional, sobre todo en punto a la protección de consumidores.

Ante el fracaso de este proyecto, el legislador europeo se ha mostrado menos ambicioso, centrando su atención en el mercado digital, poniendo al servicio del mismo todos los instrumentos necesarios para su correcto desenvolvimiento a los efectos de conseguir un incremento de la actividad económica y, por lo tanto, de la riqueza en el territorio de la Unión.
En esta línea se enmarcan las dos Propuestas de Directivas sobre las que se está trabajando, una sobre compraventa on-line[2], otra sobre contenidos digitales[3]. Esta segunda tiene por objeto, según se expresa en su artículo 1, el establecimiento de "determinados requisitos relativos a los contratos de suministro de contenidos digitales a los consumidores, en particular normas sobre la conformidad de los contenidos digitales con el contrato, los recursos en caso de falta de conformidad y las modalidades para el ejercicio de dichos recursos, y sobre la modificación y resolución de dichos contratos".

A los efectos que aquí nos interesa, esta Propuesta de Directiva sobre contenidos digitales introduce una novedad en relación con lo estipulado al respecto en CESL[4], como es regular también, en relación con la falta de conformidad y remedios, aquellos contratos llamados

[2] Propuesta de Directiva relativa a determinados aspectos de los contratos de compraventa en línea y otras ventas a distancia de bienes [COM(2015) 635 final].

[3] Propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales [COM(2015) 634 final].

[4] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una normativa común de compraventa europea COM (2011) 635 final.

"gratuitos" en los que el consumidor no queda obligado a pagar un precio, sino a la cesión de determinados datos personales. A primera vista, esto puede resultar un tanto llamativo, dado que, si el contrato es gratuito, no se entiende muy bien que el consumidor disponga de los remedios derivados de la falta de conformidad de los contenidos digitales. Para la donación no se prevén normas de saneamiento por vicios ocultos[5].

Con esta regulación, el legislador europeo trata de aunar dos intereses contrapuestos, por un lado, promover el mercado digital mediante el intercambio de datos que, sin lugar a dudas, es una fuente de riqueza. Así, se puede leer en la prensa que la intención de Bruselas es la de crear un mercado único de los datos que podría alcanzar los 84.000 millones de euros en 2020[6]. Por otro lado, se pretende proteger a los particulares que quedan amparados por la normativa de protección de datos personales[7]. Como veremos en este trabajo, el mercado de datos es un mercado suculento, en el que las empresas del sector están deseosas de participar.

Al respecto, hemos de plantearnos varias cuestiones, ¿pueden considerarse los datos personales como contraprestación a estos efectos ("counter performance" o "commodity" en terminología inglesa)? ¿Es posible negociar con datos personales, cuando su protección se considera un derecho de la personalidad?

Dejaremos la primera cuestión para un segundo apartado. Respecto de la segunda, la negociación con datos personales, presenta cierto paralelismo con la posibilidad de disponer de algunos aspectos de la personalidad, como la propia imagen, tal y como se regula en la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.[8]. Asimismo, en el ámbito anglosajón se distingue entre "right of

[5] DE CASTRO (1985, p. 264), "la tendencia a considerar especialmente las disposiciones gratuitas se manifiesta en que el donante no queda obligado al saneamiento de la cosa donada (art. 638), en que el que diera o prometiera capital al marido no queda sujeto a la evicción (art. 1397)".

[6] Diario El País, 11.1.2017 "Europa busca proteger los datos personales en el mercado digital", consultado en versión digital en http://www.elpais.com.uy/economia/noticias/europa-busca-proteger-privacidad-plataformas.html.

[7] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679.

[8] CLAVERÍA (1984, p. 43): Antes de la entrada en vigor de la CE y de la LO 1/1982 "existía una tesis prácticamente unánime acerca de cómo instrumentar la disposición sobre aspectos de la intimidad y la propia imagen (…) a través de un contrato (atípico) dotado de un régimen propuesto por la doctrina, caracterizado por un indudable rigor en cuanto al contenido y al objeto (arts. 1255, 1271, 1272 y 1275 del Código Civil), al tiempo, a la extinción y a los contratantes (…)".

CLAVERÍA (1984, p. 55): "El contrato de que se trata se regulará por las cláusulas pactadas, en cuanto no se opongan a las leyes imperativas, a la moral o al orden público (art. 1255 del Código Civil); obligará a las partes ex arts. 1091, 1256 y 1258 del mismo cuerpo legal, aunque, si se pactó una duración muy larga o no se pactó límite de tiempo, se apliquen analógicamente artículos como el 1583 (éste en cierta medida) o los 1732 y ss.; su incumplimiento generará la pertinente responsabilidad, cabiendo, en su caso, la ejecución in natura; su objeto y su causa deberán ser lícitos; en cuanto a la indagación de la llamada regla negocial, habrá que interpretar sus cláusulas con arreglo a su art. 1258 y cumpliéndolo según las reglas de la buena fe objetiva. Es cuestionable qué contratos típicos se le asemejan más, lo que cabe plantear con objeto de extraer, vía art. 4, núm. 1, del Código

publicity" y "right of privacy". El primero es el derecho de las personas públicas o celebridades de explotar comercialmente su imagen, voz, estilo u otros elementos distintivos. Se trata de un "property right" que puede ser objeto de transmisión, tanto inter vivos, como mortis causa. Por su parte, el "right of privacy" es un derecho de la personalidad, no transmisible, cuya violación genera en el ámbito del Derecho civil, la compensación de daños y perjuicios[9].

Estableciendo cierto paralelismo, podríamos pensar que el intercambio de contenidos digitales por la cesión del uso de datos personales sería un contrato atípico siempre que estuviese fundado en una causa lícita[10] y no se vulnerasen los límites de la autonomía privada. Uno de ellos sería el respecto de los derechos que las normas de protección de datos personales conceden a los particulares, como la revocación del consentimiento para el uso de los datos.

Recientemente, el European Data Protection Supervisor, en su dictamen 4/2017[11] ha manifestado ciertas objeciones a este planteamiento: "*la propuesta de directiva debería evitar las interferencias con los derechos y deberes establecidos en el Reglamento europeo de Protección de Datos Personales del año pasado. No se debería requerir a los particulares para que cedan sus datos en "pago" por un servicio en línea. Por el contrario, sus derechos e intereses deberían ser salvaguardados mediante la aplicación coherente de normas actualizadas, en ámbito de la protección de los consumidores y de datos personales*".

En consecuencia, en junio de 2017 el Consejo ha adoptado su posición sobre la Propuesta de Directiva[12], de modo que la Directiva no se aplicará cuando el proveedor trate los datos personales exclusivamente para facilitar el contenido o servicio digital, o para que el proveedor cumpla los requisitos legales a los que está sometido, y cuando el proveedor no trate los datos de ninguna otra manera. En definitiva, no se aplicará cuando el proveedor no vaya a hacer ningún uso comercial de los datos.

Asimismo, se especifica que cualquier tratamiento de datos personales en el contexto de un contrato de suministro de contenidos o servicios digitales debe cumplir la legislación de la Unión

---

Civil, soluciones inferidas de preceptos que los regulen, habiendo aludido la doctrina al arrendamiento, al mandato o, incluso –saltando a otra zona del Código-, a la constitución de un usufructo, procedimiento que no me parece demasiado fructífero, pues no creo necesario acudir a la subsunción en tipos legales para hacer operar la analogía".

[9] Véase BARNETT (2000, pp. 1225 y ss). Asimismo HIGUERAS (2001, pp. 39 y ss.)

Esta distinción se puede observar, con otra terminología en la doctrina jurisprudencial de la Sala de lo Civil del Tribunal Supremo, v. gr.: "el derecho a la propia imagen atribuye a su titular la facultad de disponer de la representación de su aspecto físico que permita su identificación, lo que conlleva tanto el derecho a determinar la información gráfica, generada por los rasgos físicos que le hagan reconocible, que puede ser captada o tener difusión pública, como el derecho a impedir la obtención, reproducción o publicación de su propia imagen por un tercero no autorizado" (STS, 1ª, 19.07.2004, Ar.5462; MP: José Ramón Ferrándiz Gabriel). Véase asimismo STC, 1ª, 16.04.2007 (72/2007; MP: Manuel Aragón Reyes), con cita de la STC, 2ª, 26.03.2001 (81/2001; MP: Carles Viver Pi-Sunyer). En sentido similar, STC, 1ª, 18.06.2001 (139/2001; MP: Pablo Manuel Cachón Villar), STC, 1ª, 22.04.2002 (83/2002; MP: Pablo García Manzano) y STC, 2ª, 28.01.2003 (14/2003; MP: Vicente Conde Martín de Hijas).

[10] Aunque los textos de armonización del Derecho europeo no se refieren a ese elemento como necesario para la conclusión del contrato o el legislador francés la haya suprimido del Código civil.

[11] Disponible en https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf. Última consulta 24.07.2017.

[12] http://data.consilium.europa.eu/doc/document/ST-9901-2017-INIT/es/pdf, última consulta 24.07.2017.

en materia de protección de datos personales y que, en caso de conflicto, prevalecerá el Derecho de la Unión en materia de protección de datos personales.

1.2. Las previsiones al respecto en la Propuesta de Directiva de contenidos digitales

En el tema que nos ocupa, la Propuesta de Directiva supone un avance en relación con CESL[13], cuyo artículo 107 limitaba los remedios para la falta de conformidad de los contenidos digitales a aquellos casos en los que el consumidor hubiese pagado un precio por los mismos, quedando solamente la posibilidad, para el resto de situaciones, de reclamar la indemnización de daños y perjuicios por los daños que los contenidos digitales "no conformes" hubiesen causado en otros elementos patrimoniales del consumidor (relatando por ejemplo, software, hardware...).

De modo diferente, el art. 3 de la Propuesta de Directiva cuando define el ámbito de aplicación de la misma, establece que tendrá lugar cuando el proveedor suministra contenidos digitales o se compromete a ello, y el consumidor paga un precio u otra contraprestación en la forma de datos personales u otros datos.

En el Considerando (14) se ofrece una explicación adicional en relación con el ámbito de aplicación de la Directiva en esta segunda modalidad, para lo que se requiere un comportamiento activo del consumidor en la revelación de información personal. Sin embargo, se excluyen los remedios cuando "el proveedor recaba datos necesarios para que los contenidos digitales funcionen de conformidad con el contrato, por ejemplo la localización geográfica cuando sea necesaria para que una aplicación móvil funcione correctamente, o con el único fin de cumplir requisitos legales, por ejemplo cuando el registro del consumidor es necesario por motivos de seguridad e identificación en virtud de la legislación aplicable".

Asimismo, debería quedar fuera del ámbito de aplicación la Directiva, cuando los datos fuesen recabados "por una *cookie*, sin que el consumidor la facilite activamente, aunque el consumidor acepte la *cookie*. De igual forma no debe aplicarse a situaciones en las que el consumidor se expone a recibir publicidad con el fin exclusivo de obtener acceso a contenidos digitales"[14]. Puesto que el mencionado Considerando limita excesivamente el ámbito de aplicación de la futura Directiva, la Comisión de Asuntos Jurídicos del Parlamento Europeo en su borrador de informe propone ampliar el ámbito de aplicación e incluir los casos en que los datos personales sean "recogidos por el proveedor o por un tercero en interés del proveedor"[15].

---

[13] SPINDLER (2016, p. 11): "Otra novedad de la propuesta (que estaba, sin embargo, ya parcialmente en el CESL) es su aplicación a los contratos de suministro de contenidos digitales a cambio de una contraprestación no dineraria en forma de datos personales o de otros datos (art. 3.1, considerando 13 PDCDig.). Aunque el contenido digital parece ser "gratuito" a primera vista, está totalmente justificado extender a esos contratos la protección al consumidor de la Directiva, porque el consumidor puede no obstante tener un interés legítimo en que ese contenido o esos servicios estén exentos de defectos y porque los proveedores no habrían ofrecido seguramente el contenido sin los beneficios que a ellos les pueden reportar los datos del consumidor".

[14] CÁMARA (2016, p.25).

[15] Cfr. Draft Report of the Committee on the Internal Market and Consumer Protection and of the Committee on Legal Affairs 7.11.2016, C80394/2015 – 2015/0287(COD) drafted by MEPs Evelyne Gebhardt and Axel Voss.

Con ello, la propuesta de Directiva supone un avance en relación con lo previsto en CESL. En la Propuesta de Reglamento de compraventa europea, siguiendo el esquema del contrato de compraventa, no se considera oneroso el contrato en virtud del cual el consumidor cede sus datos personales y, por lo tanto, no se le conceden remedios en el caso de falta de conformidad de los contenidos digitales. Sin embargo, ¿realmente se trata de un contrato gratuito?

Aquí es donde debemos plantearnos si las categorías clásicas del Derecho civil contractual encajan bien en las nuevas conceptuaciones del mercado digital.

En la ciencia jurídica moderna, el concepto de onerosidad empieza a perfilarse con la filosofía iusracionalista. Pufendorf[16]conceptúa como contratos onerosos los cuatro tipos de contratos innominados del *ius comunne*, a saber, *do ut des*, *do ut facias*, *facio ut des* y *facio ut facias*. Domat[17], por su parte, considera que en el acuerdo *facio ut des*, *do ut facias*, la causa de la obligación de uno es la causa de la obligación del otro. Con ello, incluye en el concepto de causa la interdependencia entre las obligaciones de las partes.

En esta misma línea, para Pothier[18] todo contrato debe tener una justa causa. En los contratos recíprocos, la causa de la obligación de una de las partes reside en la cosa que la otra le da o se compromete a dar. En los contratos de beneficencia, la causa reside en la liberalidad.

De este modo, en opinión de Federico De Castro, la doctrina moderna "todavía atada a sus perjuicios romanistas, y por ello de mala gana, ha tenido que recibir la distinción entre negocios onerosos y lucrativos con su implícita valoración de la causa a la manera yusnaturalista"[19].

En consecuencia, un contrato se considera oneroso cuando lleva implícitos sacrificios patrimoniales para ambas partes contratantes[20]. Por el contrario, un negocio es gratuito cuando una de las partes obtiene un beneficio sin contraprestación alguna, produciéndose un empobrecimiento en el patrimonio de la misma ("una disminución del acervo patrimonial sin compensación económica"[21]).

En los contratos de suministro de contenidos digitales, al margen de la situación en la que una de las partes asuma la obligación del pago de una cantidad de dinero, en los escenarios que aquí nos estamos planteando es posible que la parte que recibe los contenidos digitales asuma una obligación de dar (datos personales), de hacer (v. gr. observar contenido publicitario), de no hacer (no desconectar la geolocalización de ciertas aplicaciones para obtener datos que no son necesarios para la ejecución del contrato)[22].

---

[16] PUFENDORF (1672, p. 618).

[17] DOMAT (1756, p. 20).

[18] POTHIER (1825, p.24)

[19] DE CASTRO (1985, p. 260).

[20] DE CASTRO (1985, p. 262), "En su manifestación más típica, consiste en una mutua transmisión de bienes, de modo que la pérdida que para cada parte suponga se vea compensada o reemplazada patrimonialmente por el beneficio adquirido a costa de la otra".

[21] En palabras de DE CASTRO (1985, p. 260).

[22] CÁMARA (2016, p.21).

Respecto de la primera de las posibilidades, la obligación de dar datos, ¿puede entenderse jurídicamente de esta manera? ¿Son los datos elementos patrimoniales que pueden ser económicamente evaluables? En definitiva, ¿son los datos una suerte de moneda de cambio?

La protección jurídica de los datos personales es un derecho de la personalidad y por lo tanto, reúne las características propias de esta clase de derechos. La STC 292/2000 de 30 de noviembre de 2000 del Tribunal Constitucional[23] fija el contenido del derecho fundamental a la protección de datos que consiste "en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular".

La doctrina ha entendido tradicionalmente que una de las notas que define a los derechos de la personalidad es el de su carácter intransmisible[24]. No obstante, en la actualidad este carácter de la extrapatrimonialidad y no transmisibilidad de los derechos de la personalidad de modo absoluto y para todo tipo de situaciones es discutido[25].

---

[23] RTC 2000/292, MP: Don Julio Diego González Campos.

[24] Al respecto vid. MAZEAUD *et alii* (1974, p. 196): "Certain droits ont une valeur pécuniaire: ils peuvent s'a`pprécier en argent. Ainsi le droit de créance, le droit de propriété sont des droits pécuniaires. D´autres droits ont seulement une valeur morale; par exemple, le droit à une filiation déterminée, le droit de puissance paternelle, le droit à l´honneur". ALBALADEJO (2013, p. 319) distingue entre esfera jurídica de la persona y esfera no patrimonial. "La totalidad de relaciones jurídicas de que una persona es titular constituye su esfera jurídica". Dentro de ella se incluyen "dos esferas menores: 1º El formado por las patrimoniales, que son las de naturaleza económica, susceptibles, en principio, de valorarse en dinero. 2º. El formado por las no patrimoniales, también llamadas personales". En opinión del citado autor, forma parte del patrimonio de la persona el conjunto de relaciones jurídicas que en el momento de que se trate, formen parte de la anteriormente denominada esfera patrimonial. TORRENTE y SCHLESINGER (2009, p. 124) hablan de la "non patrimonialità" de los derechos de la personalidad, ya que en cuanto que tutelan valores de la persona no son susceptibles de valoración económica. LACRUZ *et alii* (1983, p. 38) se refieren a la inexpropiabilidad e inembargabilidad de los derechos de la personalidad, dado su carácter no patrimonial. Aunque se matiza que si bien no se puede disponer totalmente, es posible una disponibilidad parcial y concreta en determinados casos y para ciertos derechos. En la misma línea MONTÉS PENADÉS, *et alii* (2003, consultado en *tirantonline.com*) consideran que los derechos de la personalidad son indisponibles, "salvo ciertas disposiciones parciales y concretas, que no excluyan la titularidad para el futuro. Vgr: utilización de la imagen, disposición de alguna parte del cuerpo para ciertas finalidades (Ley 27 de octubre de 1979 sobre trasplante de órganos)".

[25] CARRASCO PERERA (2004, p. 89), se plantea el problema de la transferibilidad o enajenabilidad del contenido de los derechos de la personalidad. En su opinión "(n)o tiene mucho sentido construir, como se hace, un derecho subjetivo al honor o a la libertad o a la intimidad- o un derecho general de la personalidad que los englobe a todos- para después sostener que el contenido de estos derechos es intransmisible. Precisamente la construcción de la figura del derecho subjetivo tiene la utilidad de reservar al titular del derecho un conjunto de facultades que éste monopoliza mediante una defensa absoluta frente a terceros y que rentabiliza mediante la exclusiva del poder de disposición sobre este derecho". "La cuestión sobre la disponibilidad de los bienes de la personalidad

Existe coincidencia, empero, en torno a la idea de que tales derechos no pueden ser objeto de disposición en su totalidad, siendo posible una disponibilidad parcial.

En los derechos de la personalidad, sobre todo en los de índole incorporal (derecho al nombre, propia imagen…) puede haber intereses también de naturaleza patrimonial, como se ha visto anteriormente en la distinción entre "right of privacy" y "right of publicity" procedente de la doctrina anglosajona[26]. El régimen ordinario del Derecho contractual debería de adaptarse en aras a la protección de estos derechos de la personalidad susceptibles de comercialización[27].

No habría, por lo tanto, inconveniente en admitir, sobre la base del valor del consentimiento del titular en la disposición de estos derechos, la validez del negocio jurídico en cuya virtud el sujeto capaz haga una cesión de alguno de estos derechos a cambio de una contraprestación. Dicho contrato no vulneraría los límites del art. 1255 CC, tratándose de un contrato oneroso del que surgen obligaciones y derechos de naturaleza recíproca[28].

Respondiendo a la pregunta anterior, sobre si los datos operan como una suerte de moneda, y por lo tanto, el titular asume una obligación de dar, creo que no es éste el esquema. El objeto de las obligaciones de dar consiste en la entrega de un bien, de modo que el deber de conducta que recae sobre el deudor le impone la obligación de desprenderse del mismo, para entregarlo al acreedor. Los derechos de la personalidad, pese a que en ocasiones puedan tener un contenido

---

no se puede teorizar con carácter general ni hacerla depender de la construcción jurídica de estos bienes. En general, esta cuestión se resuelve con la aplicación de la cláusula de orden público".

MARTÍNEZ DE AGUIRRE *et alii* (2015: pp. 566-567) consideran que los derechos de la personalidad son derechos extrapatrimoniales, "en cuanto los bienes que se protegen son radicalmente personales, y carecen de contenido patrimonial. Ello no obsta a que uno de los mecanismos más característicos de reacción frente a la vulneración de estos derechos, desde el punto de vista civil, sea la concesión de una indemnización pecuniaria al titular del derecho lesionado, a fin de compensar el perjuicio que le ha causado la lesión".

"La extrapatrimonialidad de estos derechos se torna más problemática cuando el bien protegido puede tener, lícitamente, una dimensión patrimonial relevante. Es lo que ocurre, destacadamente, con el derecho a la propia imagen, que ha ido adquiriendo un valor económico y comercial importante, hasta el punto de que «hay personas que lo utilizan como herramienta de trabajo…»".

En opinión de los autores citados, p. 567, el titular del derecho no puede disponer por completo del mismo desde el punto de vista jurídico para transmitirlo definitivamente, en su globalidad, a otra persona. "Lo anterior no quiere decir, sin embargo, que el titular de un derecho de la personalidad carezca, en todo caso, de cualquier facultad jurídica de disposición en relación con ese derecho. Antes bien, es habitual admitir la existencia de una disponibilidad parcial o limitada, cuyo alcance es variable". Depende más bien del "derecho de que se trate: muy escasa tratándose del derecho a la vida, más amplia, pero todavía restringida, en relación con la integridad física"… "de mayor alcance cuando los afectados son los derechos a la intimidad y a la propia imagen".

[26] GARCÍA RUBIO, (2015, p. 244): "actualmente se cuestiona muy seriamente la extrapatrimonialidad *tout court* de este tipo de derechos, poniéndose el énfasis en el hecho de que se tras los derechos de la personalidad puede haber intereses tanto de naturaleza patrimonial como extrapatrimonial, se ha acuñado así el término "commodification" de la personalidad, como sinónimo de la construcción de ésta como mercancía; esta consideración tiene el llamado "right of publicity" del sistema norteamericano".

[27] En opinión de GARCÍA RUBIO, (2015, p. 249): "Se trata de buscar un compromiso entre el Derecho patrimonial y el deber público de proteger la dignidad humana y los derechos fundamentales".

[28] Cfr. GARCÍA RUBIO, (2015, p. 250) con cita de la STC 117/1994, de 25 de abril.

patrimonial (al margen de la esfera personal)[29] no pueden ser entendidos, de este modo, como un bien mueble por analogía, como la propiedad industrial o intelectual[30].

En el caso de la cesión de datos personales a cambio de contenidos digitales, tratándose de derechos de la personalidad, el titular del derecho sobre su información personal no puede transmitir el mismo en su totalidad ni constituir titularidades sobre las facultades que integran el derecho. Puede, sin embargo, autorizar el acceso a su esfera de exclusividad. La autorización no crea ninguna titularidad jurídica en el tercero, pero confiere licitud al acceso, independientemente de las razones que impulsen al autorizante y al autorizado[31] (v. gr. un contrato oneroso).

En mi opinión, el cedente de los datos asume una obligación de hacer, en concreto una obligación de cesión de uso de la información, del que la otra parte puede obtener un rédito. Ello de modo semejante a los contratos de cesión de los derechos sobre la imagen, siendo posible la cesión a terceros de la explotación comercial de la misma, siempre dentro de unos límites temporales y con la posibilidad de revocar el consentimiento en cualquier momento[32].

El negocio de las compañías que reciben este derecho de explotación reside, sin embargo, no en los datos de un individuo aisladamente considerado, sino en el llamado "Big data" entendido como el almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet, como tendremos ocasión de comprobar a lo largo de este trabajo.

Por otro lado, en el ámbito de los remedios, la propuesta de Directiva establece en su artículo 13.2 b), c) y d) para el caso de que el consumidor ejercite la facultad de resolución por incumplimiento del suministrador:

"b) el proveedor adoptará todas las medidas que podrían esperarse para abstenerse de utilizar las contraprestaciones no dinerarias que el consumidor haya facilitado a cambio de los contenidos digitales, así como cualesquiera otros datos recogidos por el proveedor en relación con el suministro de los contenidos digitales, incluido cualquier contenido facilitado por el consumidor a excepción del contenido que haya sido generado conjuntamente por el consumidor y otras personas que continúen haciendo uso del contenido,

c) el proveedor facilitará al consumidor los medios técnicos para recuperar todos los contenidos facilitados por el consumidor, así como cualquier otro dato producido o generado mediante el uso por el consumidor de los contenidos digitales, en la medida en que estos hayan sido retenidos por el proveedor. El consumidor tendrá derecho a recuperar los contenidos sin

[29] Cfr, STC 117/1994, de 25 de abril, en el sentido de que "cuando concurre la autorización o consentimiento de su titular, el "valor" de la imagen puede convertirse en un valor autónomo de contenido patrimonial y sometido al tráfico negocial".

[30] Sobre esta categorización vid. O'CALLAGHAN (2017, p. 196).

[31] LLÁCER MATACÁS (2012, pp. 48-61).

[32] Vid. GARCÍA RUBIO (2015, p. 252: "se mantiene desde los albores de su construcción teórica como nota característica que, tanto en los actos unilaterales como en las genuinas relaciones contractuales con prestación correspectiva, el titular del derecho de la personalidad que negocia sobre éste mantiene el derecho a revocar su consentimiento, sin perjuicio de que deba, en su caso, la indemnización por los daños y perjuicios que tal revocación pudiera causar a la otra parte".

cargo alguno, sin mayores inconvenientes, en un plazo de tiempo razonable y con un formato de datos utilizado habitualmente,

d) si los datos digitales no se hubieran suministrado en un soporte duradero, el consumidor se abstendrá de utilizar los contenidos digitales o de ponerlos a disposición de terceros, en particular eliminando los contenidos digitales o transformándolos en ininteligibles".

Ante el incumplimiento del suministrador de contenidos digitales, conforme al anteriormente transcrito artículo 13 de la Propuesta de Directiva de contenidos digitales, el consumidor tiene derecho a recuperar todos los datos subidos o producidos por él mediante el uso de los contenidos digitales. Esta obligación se hace extensible a aquellos datos que el suministrador está obligado a conservar de acuerdo con el contrato o que efectivamente haya conservado.

El suministrador, a tales efectos debería poner a disposición del consumidor de aquellos medios técnicos necesarios para recuperar los datos, todo ello, sin coste para el consumidor (pero sin que ello alcance por ejemplo, a los costes asociados a la conexión a Internet por parte del consumidor, ya que no se trata de un coste directamente relacionado con la recuperación de los datos[33]). Véase al respecto, lo que se comenta más abajo sobre la portabilidad de los datos y los problemas que puede llevar aparejado para el consumidor (el referido infra efecto "Hotel California").

En el supuesto de pago de un precio por parte del consumidor para el suministro de los contenidos digitales, en caso de un incumplimiento imparcial por parte del suministrador, el consumidor tendría derecho a resolver parcialmente el contrato en atención al período de tiempo en el que los contenidos digitales hubiesen sido conformes al contrato. En comparación, en el caso de pago mediante cesión de datos (*other tan money*), la resolución parcial no sería posible, puesto que no es factible una cesión parcial de los datos.

Lo que no regula la Propuesta de Directiva es una posible acción, ante el incumplimiento del proveedor, para obtener la restitución de las ganancias obtenidas por el suministrador del uso de los datos cedidos por el consumidor hasta el momento de la resolución[34], opción que quizá debería incluirse en la futura regulación.

1.3. Aspectos que deberían tomarse en consideración. El respeto a la transparencia

Hasta la fecha se ha considerado que el consentimiento para la transmisión de datos por el consumidor era independiente del contrato para el suministro de los contenidos digitales, sin que existiera una relación sinalagmática entre ellos. La propuesta de Directiva viene a poner fin a esta situación.

Los consumidores que contratan contenidos digitales se ven obligados a menudo a concluir varios acuerdos para el procesamiento de sus datos personales. Incluso muchas veces no es ese el nombre que se les da, sino "política de privacidad" o similar[35]. Ello es síntoma de una falta de transparencia en este tipo de contratación. Posiblemente se intuye que, aunque estos servicios se

[33] RADLEY y BEALE (2016, p. 805).

[34] METZGER (2017, p. 7).

[35] Véase WENDEHORST (2016, pp.189 y ss.)

ofrecen como "gratuitos", la cesión de datos personales opera como una suerte de contraprestación[36].

Esta forma de contratación, estandarizada, precisa del respeto a un principio fundamental cual es el de la transparencia. Compartir información puede ser una forma de promover la toma de decisiones de un modo responsable y de empoderar a los ciudadanos.

El principio de transparencia se presenta como un valor en alza en este tipo de contratación. Un mercado transparente proporciona tanta información como es posible a todos los participantes en el mismo, lo que provoca que se minimicen las ventajas informativas de otros participantes[37]. Con lo que es un principio económicamente eficiente.

En España, algunas sentencias recientes del Tribunal Supremo han considerado que una cláusula contractual es abusiva, no solo cuando existe un desequilibrio contractual, sino también, cuando existe una falta de transparencia[38]. Las cláusulas contractuales no son transparentes cuando los consumidores no son capaces de prever las consecuencias económicas y las cargas legales que se derivan del contrato.

Aplicando este deber de transparencia a este ámbito de la contratación, el consumidor debería ser informado de que efectivamente la cesión de sus datos personales va a operar como una contraprestación por estos servicios. Asimismo, cumpliendo con el Reglamento europeo de protección de datos (arts. 6 (1) a y 9 (2) a), el suministrador debería informar al consumidor, antes de que éste quede vinculado por el contrato, sobre su derecho de revocación del consentimiento necesario para el procesamiento de sus datos personales, así como los efectos que tal revocación tendrán en el ulterior desenvolvimiento del contrato. Esto puede provocar un problema, puesto que en la dogmática contractual tradicional se desconocen los contratos sinalagmáticos en los que una de las partes tiene derecho a revocar su consentimiento[39]. Aunque se puede encontrar cierto paralelismo con el art. 2.3 Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen según el cual: "El consentimiento a que se refiere el párrafo anterior será revocable en cualquier momento, pero habrán de indemnizarse en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas". Se trata de una situación excepcional (justificada por verse afectados derechos de la

[36] METZGER (2017, p. 3), se refiere a un estudio realizado al respecto en Alemania, donde muchos usuarios de estos servicios eran conscientes de que la cesión de datos equivalía a una suerte de contraprestación en estos servicios "gratuitos".

[37] LINDQVIST (2012), pp. 99 ss.

[38] Sobre el control de transparencia véase SSTS Sala 1ª del Tribunal Supremo 18 de junio de 2012 (Ar. 4183, MP: Jose Antonio Seijas Quintana), SSTS Sala 1ª del Tribunal Supremo 9 de mayo de 2013 (Ar. 1916, MP: Rafael Gimeno-Bayon Cobos), SSTS Sala 1ª del Tribunal Supremo 8 de septiembre de 2014 (Ar. 3903, MP: Francisco Javier Orduña Moreno), SSTS Sala 1ª del Tribunal Supremo 24 de marzo de 2015 (Ar. 1279, MP: Rafael Saraza Jimena) y SSTS Sala 1ª del Tribunal Supremo 25 de marzo de 2015 (Ar. 1280, MP: Eduardo Baena Ruiz). Asimismo, SSTJUE 21 de marzo de 2013 (C-92/11, MP: M. Safjan), SSTJUE 30 de abril de 2014 (C-26/13, MP: A. Prechal) y SSTJUE 26 de febrero de 2015 (C-143/13, MP: A. Prechal).

[39] En la doctrina alemana sucede lo mismo, como plantea METZGER (2017, p. 6).

personalidad), puesto que esta facultad de revocación afecta al principio de obligatoriedad de los contratos (art. 1256 CC)[40].

Igualmente, habría de ser informado sobre los destinatarios de sus datos personales (conforme al art. 13 del Reglamento). Al respecto, deberían considerarse abusivas, por ejemplo, las cláusulas predispuestas en las que el suministrador se reservase el derecho a alterar la finalidad que se observó en el momento de recabar el consentimiento para el tratamiento de los datos, sin informar al consumidor[41]. En esta línea, los tribunales alemanes han fallado repetidamente en el sentido de considerar abusivas las cláusulas contractuales si la finalidad para la que se requirió el consentimiento para el tratamiento de los datos había sido redactada vagamente y con un lenguaje complicado[42].

2. La invasión del Big data

2.1. Introducción

Sólo en 2014 se calculó que, en un minuto en Internet, se generaron 4,1 millones de búsquedas en *Google*, se escribieron 347.000 twitts, se compartieron 3,3 millones de actualizaciones en *Facebook*, se subieron 38.000 fotos a Instagram, se visualizaron 10.000.000 de anuncios, se subieron más de 100 horas de vídeo a YouTube, se escucharon 32.000 horas de música en streaming, se enviaron 34.700.000 de mensajes instantáneos y se descargaron 194.000 Apps[43]. En un solo minuto se transfirieron más de 1.570 terabytes de información en Internet.

A la velocidad a la que se expande la tecnología, en pleno 2017, estas cifras se han incrementado exponencialmente.

Cada uno de esos movimientos en la red genera información que se digitaliza en código binario y se almacena masivamente para, con técnicas de lo más complejas, analizarlos y extraer nuevas referencias que en el futuro puedan aplicarse a la transformación del mundo real. Llamamos pues Big data al almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet.

En la globalización del siglo XXI, las innovaciones tecnológicas junto con el nuevo modelo económico y social, han hecho proliferar enormes cantidades de bases de datos relativos a realidades tangibles (datos físicos) o intangibles *a priori* pero convertidos mediante algoritmos en

[40] Cfr. STC 25 de abril de 1994 (Ar. 117, MP: José Gabaldón López): "Mas, en esos supuestos de cesión voluntaria de la imagen o de ciertas imágenes, el régimen de los efectos de la revocación (prevista en el art. 2.3 de la L.O. 1/1982 como absoluta) deberá atender a las relaciones jurídicas y derechos creados, incluso a favor de terceros, condicionando o modulando algunas de las consecuencias de su ejercicio; y corresponde a los Tribunales ordinarios la ponderación de los derechos en conflicto en tales casos, sin perjuicio de la que a este Tribunal compete, únicamente desde la perspectiva constitucional" .

[41] LOOS (2013, pp. 611 y ss).

[42] METZGER (2017, p. 5).

[43] Estudio elaborado por la Online Business School de la Universidad de Barcelona, última consulta 23.06.2017, www.obs-edu.com.

información digital. Entre los unos y los otros hay un número descomunal de datos de carácter personal.

Estos bancos de datos contienen información relativa a nuestra identidad (nombres, lugar de residencia, profesión, estado civil, propiedades…) así como otra información personal tan diversa como nuestra religión, ideología, clase social, salud… La información, en el primer caso, se obtiene de registros públicos o privados y por ello podíamos decir que es "real" mientras que, en el segundo caso, ésta es obtenida a través de otros parámetros -no siempre fiables- como nuestras pautas de comportamiento, preferencias culturales o patrones de consumo.

Ambos tipos de información quedan almacenadas en enormes bases de datos y unos y otros permiten identificarnos o reconstruir nuestra identidad. Este proceso, llevado a cabo masivamente por parte de las empresas de telecomunicaciones, sumado a los datos generados por las Administraciones públicas y las industrias privadas de seguridad, es lo que se ha denominado por algunos autores como *Dataveillance,* o dicho de otra forma: la normalización social de la cultura de la vigilancia.

Pero no sólo se trata de acumular datos y datos, sino de interrelacionarlos entre sí para lograr aumentar exponencialmente la información a obtener y sacarle así un mayor partido. Es lo que SOLOVE[44] llama *agregación*: conformar el perfil de una persona a través de la triangulación y organización de la información que se ha obtenido sobre ella, obteniendo así nuevos datos sobre un individuo. Este proceso, al alterar las expectativas de las personas, supone una amenaza para la intimidad, ya que el sujeto no tiene el control del conocimiento que se está obteniendo a través de su información personal.

Para la filtración de los datos (lo que se conoce como *data mining*) hay software específicos que se encargan de cruzarlos atendiendo a los parámetros que para su finalidad concreta resulte interesante y la información obtenida vuelve a almacenarse de nuevo en otras bases de datos, compartimentadas según los criterios empleados y a las que llamamos bancos de datos. Unos mismos datos pueden clasificarse según distintos parámetros y, en consecuencia, pueden formar parte de infinidad de bases de datos.

Internet ha logrado aumentar exponencialmente el tráfico de información y, a través de la interconexión mundial de bases de datos y la cantidad de copias de las mismas, podemos afirmar que el tráfico de información en Internet es hoy en día imparable. Esto en sí mismo no es negativo, gracias a ello tenemos acceso a una cantidad enorme de fuentes de casi cualquier parte del Mundo que de otro modo sería impensable, ¿la otra cara de la moneda? la falta de privacidad[45] de los ciudadanos.

[44] SOLOVE (2006, pp. 477 y ss.).

[45] Nótese que se habla de privacidad y no de intimidad, utilizando una nomenclatura más próxima a la tradición jurídica del *common law* y no tan acorde con nuestro ordenamiento jurídico. A lo largo de este trabajo se usará el término privacidad de forma consciente y precisamente para hacer notar al lector que los datos personales pueden tener incidencia en el espacio "privado" de la persona más allá de su intimidad. Es decir, se pretende poner de manifiesto que, si bien todas las conductas que aquí se describen no afectan a la intimidad estricta de la persona (en el sentido doctrinal más tradicional y consolidado) sí que tienen incidencia en una esfera menos íntima pero igualmente privada y, por ende, lesiva de determinados derechos y libertades).

Este proceso, además, es difícilmente reversible. En el que podemos llamar nuevo Internet de los datos[46] éstos se usan, se reutilizan, se vuelven a usar sus desechos y raramente se destruyen, cancelan o desaparecen; sino que se almacenan porque en el futuro serán objeto de nuevos usos.

Una vez los datos son incorporados a Internet, circulan libremente por el ciberespacio pasando de unas bases de datos a otras y de un servidor de Internet a otro por lo que, si además tenemos en cuenta las copias periódicas que se hacen de las páginas web, aunque se consiga borrar la información de su fuente original, es prácticamente imposible hacerla desaparecer de todos los rincones del ciberespacio. Esto ha sido bautizado por el Prof. TRONCOSO como el "efecto Hotel California": *you may enter, but you may never leave*[47].

2.2. Regulación. Hecha la Ley, hecha la trampa

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)[48] regula el registro, el tratamiento y toda modalidad de uso posterior de esos datos por los agentes públicos y por empresas privadas y para ello articula algunos principios de actuación así como una serie de mecanismos que permiten a los ciudadanos ejercer sus derechos, por ejemplo, de acceso, rectificación y cancelación de su información personal contenida en algunos de estos ficheros. La LOPD, como no podía ser de otra manera, se basa en el consentimiento que el afectado por el tratamiento de dichos datos debe prestar en todo momento, así como en la información clara y detallada que previamente debe recibir para consentir.

Sin embargo, ¿cuántos de nosotros hemos leído las 30 páginas en las que constan los usos y términos del servicio antes de instalar la aplicación *WhatsApp*? Pues eso. Y, de haberlo hecho, es muy posible que la mayoría de los destinatarios no comprendiesen todos los pormenores. Las empresas están obligadas a detallar de forma comprensible su política empresarial y nosotros a leerla detenidamente, sin embargo, partimos de premisas totalmente falsas.

En cualquier caso, nosotros decidimos instalarnos una aplicación como *WhatsApp* sin leer antes las condiciones de privacidad y con ello aceptamos, entre otros, ceder a *Facebook* y a sus empresas asociadas nuestros números de contacto, nuestra foto de perfil o nuestra geolocalización, para fines aún sin detallar.

El oscurantismo con que se llevan a cabo estas prácticas empresariales es más que deplorable como también lo son las cláusulas abusivas de contratación y ni qué decir tiene la modificación unilateral de las mismas. Pero además de las cláusulas ambiguas nos encontramos ante un problema de jurisdicción y es que, a pesar de operar en nuestro país, la mayoría de proveedores de servicios de Internet se encuentran en suelo americano, un "paraíso de privacidad" cuya legislación ampara la mercantilización de los datos personales, lo que ha supuesto en la practica

[46] Véase NAVAS (2016, p. 29).

[47] TRONCOSO (2010, p. 43).

[48] BOE nº 298, de 14.12.1999.

un éxodo masivo de estas empresas hacia la jurisdicción estadounidense[49], que acoge éstas y otras prácticas empresariales de dudosa legalidad, al menos, en suelo europeo.

Una de las principales novedades introducidas por el reciente Reglamento Europeo de Protección de Datos[50], que pese a estar ya en vigor será plenamente aplicable el 25 de mayo del próximo 2018, es precisamente acabar con esta falta de territorialidad que impide la actuación del poder judicial, al disponer que su normativa será también de aplicación al tratamiento de datos personales de personas residentes en territorio europeo "por parte de un responsable o encargado no establecido en la Unión" cuando ofrezcan sus servicios en ella, acabando por fin con el argumento esgrimido por la mayoría de corporaciones internacionales que acostumbran a alegar la falta de aplicabilidad del Derecho europeo para eludir sus obligaciones, obligando además a los ciudadanos a pleitear en tribunales estadounidenses.

El nuevo Reglamento pretende dotar a los ciudadanos de un mayor control de sus datos personales por lo que obliga a las empresas a una serie de actuaciones en consecuencia, entre otros: mantener un registro del tratamiento de datos, realizar evaluaciones de impacto, establecer códigos de conducta, nombrar un delegado de protección de datos… haciéndoles responsables activos en la gestión de la información personal.

Además, se ha reconocido el derecho a la portabilidad de los datos de forma que todo usuario podrá solicitar que se retire de Internet sus datos personales que ya no son necesarios para la finalidad con la que fueron inicialmente recogidos, incluso si se tratase de informaciones obsoletas o irrelevantes.

A pesar de que el nuevo Reglamento Europeo comprende novedades interesantes y goza de buenas intenciones, lo cierto es que la tecnología en sí 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.

También, sería ingenuo pensar que el objetivo último de este nuevo marco legal es proteger la privacidad de los ciudadanos frente a la tiranía de las operadoras de Internet, pues la intención subyacente de esta norma es justo la contraria: dejar de obstaculizar el mercado interior de la Unión Europea que está dificultando el ejercicio de actividades económicas a escala comunitaria, provocando un falseamiento de la competencia.

Conviene recordar en este punto, lo acontecido con el *Safe Harbor* y la Sentencia del TJUE de 2015

[49] Un ejemplo de ello lo encontramos en la polémica inauguración en el año 2014 del centro de datos más grande del Mundo (equivalente a quince estadios de fútbol) a manos de la Agencia de Seguridad Nacional de EE.UU para el análisis de los mismos, última consulta 3.04.2017,

http://www.bbc.com/mundo/noticias/2012/03/120326_mayor_centro_espias_eeuu_fp.shtml?print=1.

[50] Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE nº 119, de 4.5.2016.

en el caso Schrems[51] que lo declaró inválido. La regulación europea en materia de protección de datos anterior al vigente Reglamento, prohibió la transferencia internacional de datos personales de ciudadanos europeos a países que no contasen con ciertos estándares de protección, entre ellos, Estados Unidos. Entonces, ¿cómo operan empresas como *Facebook*?

Para lograr el intercambio comercial de datos entre la Unión Europea y los Estados Unidos entró en vigor el año 2000 el *Safe Harbor* (Puerto Seguro), una norma de adhesión voluntaria a la que se suscribieron empresas que operaban con datos a los dos lados del atlántico para garantizar así el tráfico de los mismo, a cambio de prometer el cumplimiento de ciertas normas de seguridad[52].

A raíz de las filtraciones llevadas a cabo en 2013 por Edward Snowden, excontratista de la NSA y la CIA, se dejaron en evidencia las prácticas de espionaje masivo que se estaban llevando cabo por agencias de EE.UU. -en colaboración con otros países aliados- sobre la población mundial[53]. Esto llevó al TJUE, a raíz de una demanda presentada por un ciudadano austríaco que arremetía contra *Facebook* por vulnerar su privacidad, a concluir que Estados Unidos no era un país seguro en materia de privacidad, abriendo la puerta a los estados europeos a que declarasen, si así lo estimaban, que el tratamiento de datos de sus ciudadanos por EE.UU. era ilegal.

¿Entonces ya no se transfieren datos personales desde la UE hacia EE.UU.? Por supuesto que sí. Aunque el nuevo Reglamento Europeo de Protección de Datos endurece los estándares de seguridad, por otro lado, Estados Unidos y la Unión Europea ya han llegado a un nuevo acuerdo llamado *Privacy Shield* (Escudo de Privacidad) que, aunque impone mayores exigencias a las compañías estadounidenses, les permite de facto seguir especulando con los datos personales de los ciudadanos europeos con cierta impunidad. En definitiva, la transferencia internacional de datos se está convirtiendo en la regla general y no en la excepción.

Lo cierto es que partimos de tradiciones jurídicas antagónicas en materia de privacidad. Mientras que la legislación europea contiene mayoritariamente normas más proteccionistas en términos de privacidad, en Estados Unidos, dónde tienen origen y domicilio las principales empresas que operan en el ámbito de Internet, apuestan por rentabilizar al máximo la información personal de los ciudadanos y tratan de eliminar todo obstáculo para su comercialización, lo que pasa por liberalizar el sector y forzar la autorregulación.

En consecuencia, las líneas jurisprudenciales también resultan contrarias, de hecho en las sentencias más relevantes en materia de privacidad de los últimos años la mayoría de los demandantes han visto rechazadas sus pretensiones mientras que se ha considerado que las empresas que recaban, tratan y venden a terceros los datos personales de sus clientes actúan con

---

[51] Sentencia de 16 de octubre de 2015, asunto C-362/14 (MP: T. von Danwitz), disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=105220.

[52] Los requisitos que se exigían para formar parte del *Safe Harbor* eran mínimos, mucho menos rígidos que los exigidos por la normativa europea de protección de datos, por lo que casi cualquier empresa estadounidense que lo solicitase entró a formar parte de él. Se puede consultar la lista completa en: https://safeharbor.export.gov/list.aspx. Última consulta 11.06.17.

[53] http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm. Última consulta 29.05.17.

pleno respeto a la legalidad.

Así, en el famoso caso *Dwyer v. American Express*, se planteó una demanda por invasión de la privacidad por parte de los clientes de American Express al saberse que ésta cedía información relativa a sus hábitos de consumo y que eran categorizados en función de la cantidad récord de gasto, sus adquisiciones mensuales, su comportamiento de compras e incluso sus historiales de consumo. La Corte de Apelación de Illinois[54] rechazó la demanda negando que existiera un acto no autorizado de intrusión ya que "usar la tarjeta American Express es voluntario" y esto inevitablemente revela a la empresa los hábitos de consumo de su titular así como sus preferencias de compra, información libremente dada que simplemente por ser compilada o vendida a terceros no consiste en un acto ilegal.

La jurisprudencia americana ha considerado que sólo hay ilegalidad cuando el nombre o la imagen de un cliente se hace pública con la intención de demostrar que respalda un producto o servicio, rechazando el resto de las demandas que planteen la apropiación o explotación de la personalidad, al entender que no hay base suficiente en el derecho de propiedad para exigirlo[55]. Su argumento se basa en que la propiedad de los datos personales pertenece a quién los colecta y almacena no existiendo, por ejemplo, derecho de propiedad en los nombres propios por lo que, incluir un nombre en una lista de correo para fines publicitarios no es contrario a la Ley por no constituir un ejercicio de dominio o explotación del mismo ni privar a una persona de la posesión de su nombre[56].

Es decir, desde la óptica americana, la información personal no es propiedad de nadie hasta que ésta no se recolecta, lo que supone una contradicción ya que identifica la propiedad con el valor económico cuando ambas cosas no tienen por qué ir aparejadas. La información personal no resulta protegida de ningún modo por los tribunales de EE.UU. que valoran la legalidad de una conducta en base a "una expectativa razonable de privacidad" lo que, obviamente, varía en función de diferentes factores sociales, económicos o culturales.

Por motivos como estos, se explica el fallo del TJUE en la sentencia Schrems -que anuló la decisión de la Comisión Europea que declaraba Estados Unidos como "puerto seguro" y confirmó que el criterio de las autoridades nacionales de Protección de Datos está por encima del Ejecutivo comunitario y de sus acuerdos con terceros estados cuando pueda existir riesgo para la protección de la información de los ciudadanos- y obligan a recibir con escepticismo acuerdos como el *Privacy Shield*.

Lo cierto es que no contamos con un instrumento jurídico internacional único, de carácter vinculante, que permita actuar en cualquier lugar del mundo cuando un derecho fundamental como la intimidad, se vea menoscabado. Y de esta falta de jurisdicción (y de territorialidad también pues Internet, por definición, carece de espacio físico) no se benefician los ciudadanos individuales, sino que es aprovechado por las empresas que controlan el mercado de Internet para hacer negocio y obtener rendimientos económicos de nuestros datos personales.

---

[54] *Dwyer v. American Express Company*, 652 N.E.2d 1351, 1995 (MP: Edward C. Hofert).

[55] *Shibley v. Time, Inc.*, 341 N.E.2d 337, 1975 (MP: J. Fink).

[56] *Avrahami v. U.S. News*, 95-7479, 1996 (MP: William T. Newman).

Las normas sobre protección de datos parecen *a priori* incompatibles con la forma de proceder en el Internet de las cosas y de los datos masivos. Mientras que tales leyes, en nuestro caso la LOPD, exigen el consentimiento inequívoco del titular de los datos personales que deberá de conocer expresamente la finalidad del tratamiento de sus datos, así como autorizar la cesión de éstos a terceros, en el ámbito de Internet y las empresas que operan en él, es prácticamente imposible saber cuándo estamos siendo monitorizados y qué usos posteriores se le va a dar a nuestra información más personal.

Frente a esta situación hay quienes defienden la autorregulación como instrumento de control pero, a tenor de los acontecimientos, no parece que sea una buena idea, al menos no para los ciudadanos y la salvaguarda de sus derechos.

El error de partida del *soft law* es que, pese a que usar servicios de Internet es voluntario, una vez decides hacerlo, las reglas de juego se imponen unilateralmente por parte del proveedor del mismo, donde las condiciones de uso son auténticas cláusulas contractuales de adhesión. Los usuarios y los prestadores del servicio no están en igualdad de condiciones, así como los titulares de los datos personales que allí se manejan no son sus propietarios.

Las reglas de juego en Internet no son las mismas que en el mundo real, aunque las consecuencias que comportan las vulneraciones de derechos transciendan a la realidad offline.

3. El negocio de la privacidad

3.1. Los datos personales, el nuevo petróleo

En la actualidad podemos hablar de una expropiación de la privacidad sin precedentes en nuestra tradición jurídica pues: los datos personales se han convertido en un activo patrimonial de gran valor económico en el mercado, el petróleo del siglo presente, ellos orientan el desarrollo y uso de nuevos productos y servicios.

La obtención de información personal cuenta con dos grandes aliados, de una parte las nuevas herramientas tecnológicas y, de otra, la fragmentación legislativa o incluso la desregulación, lo que da rienda suelta al mercadeo de datos personales sin demasiados problemas.

Estos dos factores han convertido a la privacidad en el producto estrella a comercializar por las grandes corporaciones del Big data. El negocio resulta más que rentable: los usuarios ceden gratuitamente sus datos personales (a cambio de la instalación de una App, mediante la suscripción a un boletín de ofertas de un grupo empresarial, permitiendo la geolocalización del Smartphone, revelando todo tipo de información personal en una red social…) a empresas que se dedican a almacenarlos, venderlos a terceros o procesarlos para un tratamiento posterior, generalmente con objetivos de marketing.

Los usuarios de estos servicios ya no somos meros consumidores pasivos sino que, a través de una pérdida considerable de nuestra privacidad, nos hemos convertido en parte del producto cuya ganancia, sin embargo, no percibimos. Sin ser del todo conscientes hemos evolucionado del Internet de las cosas al Internet de las corporaciones, donde las cosas somos nosotros y en el que

los datos personales son el nuevo producto a comercializar[57].

3.2. Los *Data Brokers*, los mercaderes de la privacidad

El Big data de una empresa puede llegar a ser su activo más valioso y juega un papel muy importante en la toma de decisiones de mercado. ¿Y quién compra nuestros datos? Los *Data Brokers* son empresas que se encargan directamente de hacer negocio con nuestra información, son vendedores de información que se dedican a recolectar datos de los consumidores (la mayoría de veces sin su consentimiento) y vendérselos a un tercero. Pese a que el mercado es opaco y actúan básicamente en la clandestinidad, se calcula que estas empresas no llegan ni a la decena pero, en cambio, controlan todo el tráfico de Internet[58].

Estos datos se filtran, analizándolos y cruzándolos, hasta crear catálogos con perfiles o patrones de comportamiento y posteriormente se venden a otras empresas que los usaran, por ejemplo, para verificar identidades, detectar fraudes, pero, sobre todo, para fines publicitarios.

¿Cómo llevan a cabo su actividad? Recogen información tanto de fuentes públicas (Hacienda, Registro Mercantil, DGT…) como privadas (cookies, redes sociales, tarjetas de fidelización…) y gracias a ellas obtienen datos no sólo acerca de cómo nos llamamos o dónde vivimos, sino que son perfectamente capaces de averiguar qué compañía aérea preferimos para viajar, el tipo de cine que solemos ver, la asiduidad con la que visitamos determinados videos de YouTube, el presupuesto de nuestras futuras vacaciones, las enfermedades que hemos padecido, si estamos pensando en cambiar de coche…

El marketing personalizado no es nada nuevo pero la tecnología ha abierto nuevas vías de explotación y los *Data Brokers* están haciendo negocio con éstas. Sus últimas prácticas consisten en la instalación de sensores en lugares estratégicos, como por ejemplo centros comerciales, capaces de monitorizar la señal WiFi de nuestros Smartphones, de este modo saben en qué tiendas compramos, en qué escaparates sólo nos fijamos, cuánto tiempo dedicamos a ello… y así retratan nuestros hábitos de consumo. No cabe duda de la revolución que para la mercadotecnia esto supone y de cómo esta información es de gran valor para muchas empresas[59].

---

[57] DEL FRESNO (2014, pp. 107-110).

[58] Un informe de 2013 de la Comisión Federal de Comercio del Senado de los Estados Unidos (*Federal Trade Comission*) identificó a nueve empresas como *Data Brokers*, a las que sacó del anonimato para alertar del peligro que supone esta mercadotecnia. El informe disponible, en inglés: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. última consulta 22.05.17.

[59] En algunos casos incluso, mediante este uso de la información personal, se producen prácticas comerciales desleales ya que, empleando de forma sesgada la información personal de usuarios, se elaboran campañas de marketing dirigidas a explotar psicológicamente el consumidor con la intención de influir en su capacidad de decisión y en su comportamiento económico, tratando de imponerle preferencias respecto de la contratación de determinados bienes o servicios.

3.3. Los ciudadanos contribuimos al negocio regalando nuestros datos personales

Si bien es cierto que parte de la información personal que se encuentra en bases de datos no cuenta con nuestro consentimiento o nuestro conocimiento, hay mucha otra información que es revelada conscientemente por los directamente "afectados" mediante tarjetas de fidelización, suscripciones gratuitas, obtención de cupones de descuento…

Como si de vender el alma al diablo se tratara, cedemos nuestra biografía digital a cambio de servicios gratuitos, desde el historial de búsqueda hasta nuestras preferencias políticas, pasando por nuestra localización. Cada vez que *Google Now* nos indica el tiempo que nos queda para llegar a casa, lo hace porque sabe dónde vivimos, dónde está nuestro trabajo, cuáles son nuestros horarios e incluso a qué velocidad media solemos desplazarnos.

Algunas veces por pura pereza, no cambiamos la configuración de fábrica de nuestros dispositivos, no leemos las condiciones generales de contratación o no desmarcamos las casillas que permiten usar nuestros datos para "recibir ofertas o descuentos", otras veces sí que se nos exige una conducta más proactiva al requerirnos enviar cartas (¡en pleno 2017!) a un apartado de correos para manifestar nuestra oposición al tratamiento de datos que se aplica por defecto. Por no hablar de la información que puede extraerse de las redes sociales, con un breve vistazo al perfil de usuario podemos saber la ciudad en la que vive una persona, dónde y con quién estudió, cuál es su situación sentimental, sus gustos musicales, sus tendencias políticas, sus preferencias de ocio…

Todo esto se debe al desconocimiento o quizás indiferencia del usuario de lo que se hace con toda esta información. La masificación de las redes sociales ha supuesto una nueva era de sobreexposición que los expertos han convenido en llamar "extimidad", como concepto clarificador de este cambio de paradigma en la privacidad. Lo curioso es que esta extimidad está suponiendo la vulneración de nuestros derechos, muchas veces por la renuncia del propio titular. Renunciamos a nuestra privacidad para tener una cuenta en *Facebook*, para que *Google maps* nos diga qué camino es el más rápido para llegar a casa, para que la compañía hotelera nos aplique un 10% de descuento sobre el precio… y así nos damos cuenta de que en el mundo online no tenemos intimidad ninguna.

La información que se revela en muchos casos puede parecer inofensiva, pero no es disparatado pensar que en algún momento pueda resultar perjudicial para la persona en concreto, aunque sea en términos de reputación online que se añade hoy a nuestra biografía[60]. En Internet, el tiempo siempre es lineal: el pasado sigue estando presente y será siempre accesible en el futuro.

El avance imparable – y la mayoría de veces positivo, no puede negarse- de las nuevas

[60] Precisamente estos días se ha hecho pública la condena penal por parte de la Audiencia Nacional a Cassandra Vera, una joven de 21 años que hace más de cinco hizo comentarios irónicos y humorísticos en su perfil Twitter acerca de Carrero Blanco (Sentencia nº 9/17 de 29 de marzo, de la Audiencia Nacional. Ar. 514, MP: Juan Francisco Martel Rivero). Sin entrar a comentar la desproporcionalidad de dicha Sentencia, es innegable que la reputación online se añade hoy a nuestra biografía y que, por tanto, estamos más expuestos públicamente. En este caso en concreto, Cassandra ha sido condenada a un año de prisión y a siete de inhabilitación absoluta lo que, en su caso, le ha comportado graves perjuicios económicos y profesionales.

Fuente: https://politica.elpais.com/politica/2017/03/29/actualidad/1490788774_203770.html.

tecnologías no tiene porqué ser inversamente proporcional a la vulneración del derecho a la intimidad de sus usuarios, y desde luego no es excusa suficiente para quebrantar derechos fundamentales.

3.4. ¿Cuánto valen nuestros datos personales?

Las nuevas formas de explotación económica que permite el mercado digital, como la propia vida moderna, están llenas de contradicciones. Si como se ha visto, a medida en que aumenta la demanda de los servicios gratuitos que necesitan de nuestros datos personales para su funcionamiento incrementa también la preocupación por la privacidad, otra paradoja se produce en torno a este fenómeno. Y es que, mientras que empresas como *Facebook* o *Google* ganan millones de dólares a partir de los ingresos que obtienen de los anunciantes a los que venden nuestros datos personales, la estimación del valor que se deriva de éstos en relación a cada uno de los usuarios es más bien baja.

Se calcula que los usuarios estiman su información personal online entre los 2.000€ y los 3.000€, un valor desorbitado si tenemos en cuenta el precio que un anunciante pagaría por usarla: unos céntimos de euro[61].

Todos los datos personales tampoco son igual de valiosos, el mercado digital no cotiza igual nuestra localización que nuestro nivel de estudios. De entre toda esta información, la que tiene un valor económico superior es la relativa a la salud cuyos datos, especialmente sensibles por razones obvias, cotizan al alza en el mercado negro[62].

Es muy difícil calcular el valor de nuestra información personal, en primer lugar, por la falta de datos al respecto, pues es un mercado opaco lleno de secretismo y dónde las fluctuaciones económicas del producto escapan a nuestro entender. No obstante, se han llevado a cabo diversas estimaciones, como la que realizó el *Financial Times*[63], creando una calculadora digital para poner valor a nuestra información personal mediante la realización de un test. Según los resultados, la información básica como la edad, el sexo y la ubicación tendrían un valor de 0,0005$ mientras

[61] 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 02.06.17.

[62] Los ciberdelincuentes se están especializando cada vez más en el robo de datos de hospitales, farmacéuticas y asegurados de salud, de hecho, el sector sanitario ha sido el más afectado por ataques informáticos destinados al robo de información sensible. Como ejemplo, el pasado febrero se produjo un ciberataque al Hollywood Presbyterian Medical Center de los Ángeles robando los historiales médicos de sus pacientes así como los correos electrónicos de sus trabajadores, por el que se solicitó un rescate de 3,7 millones de euros. Lo mismo ocurrió ese mismo mes en dos hospitales alemanes, el Lukas Hospital y el Klinikum Arnsberg Hospital, ambos sufrieron el ataque de un virus informático en su sistema que bloqueó los archivos exigiendo dinero para liberar los datos previamente cifrados. Fuentes de las noticias disponibles, respectivamente, en https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center y http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030 . Última consulta 02.06.17.

[63] Herramienta disponible en http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4g6IgV7zg. Última consulta 03.06.17.

que si se añade más información como la marca de coche que usamos, dónde nos vamos de vacaciones o información financiera, esta cifra aumentaría exponencialmente.

No obstante, el hecho que nuestros datos personales singularmente considerados tengan un valor relativamente bajo, no implica que su explotación global por parte de empresas como *Google* o *Facebook* no les esté reportando numerosos beneficios económicos.

Esto se debe, en segundo lugar, a que el valor de la información personal varía en función del volumen de datos que se comercialice, cuanta más información y cuantas más variables al respecto, mayores son los ingresos[64].

Los datos de cada persona no son en sí los más relevantes, lo más valioso es obtener información sobre la totalidad de nuestra actividad online que permita rastrear nuestras reacciones, pautas y preferencias y catalogar así nuestro patrón de comportamiento en base a una visión comercial. Así, los datos individualmente considerados van cobrando relevancia en la medida en que se cruzan con otros datos y permiten una reconstrucción de la personalidad online capaz de predecir nuestros pasos o intereses en la vida real.

Un aspecto a tener en cuenta es que no todos los bancos de datos tienen un destino comercial, la información personal se vende como cualquier otra mercancía, a quien tenga interés y dinero para comprarla con independencia de la finalidad que vaya a darle, precisamente este es el riesgo más inquietante de especular con la privacidad. Así, por ejemplo, en el mercado negro, hoy en día un historial clínico tiene más valor que una tarjeta de crédito.

Recientemente la prensa se hacía eco de *Exact Data*, una empresa *Data Broker*, que cuenta con un banco de datos de más de 200 millones de contactos de Estados Unidos y que se pueden filtran entre más de 450 categorías, entre ellas algunas tan sensibles como religión y etnia, además de contar con otras categorías preconfiguradas como "estadounidenses hispanos no asimilados". Es más, dicha empresa publicita la oferta de los datos de 1,8 millones de musulmanes por 126.851€, a razón de 7 céntimos de euro por persona.

Esta posibilidad, ilegal en países como el nuestro pero cuyo reproche de moralidad va más allá de nuestras fronteras, pone en peligro derechos fundamentales de los más básicos como la intimidad o la prohibición de discriminación, cosa que ya han puesto de relieve algunas organizaciones en defensa de los derechos humanos[65].

Si comercializar con estos datos para meros propósitos de marketing ya suscita dudas más que razonables, éstas aumentan conforme imaginamos los numerosos usos que pueden darse a los mismos en manos equivocadas, con propósitos claramente discriminatorios y vulneradores de derechos.

---

[64] Investigadores de la Universidad de Carlos III de Madrid han desarrollado "FDVT: Facebook Data Valuation Tool", una herramienta para saber cuánto dinero gana *Facebook* con los datos personales de sus usuarios. Así, mientras se está utilizando *Facebook*, aparece una ventana en la que se detallan los ingresos que genera el usuario a dicha red social mientras se navega por ella, en tiempo real y en relación al valor económico de la publicidad. Éstos van aumentando a medida en que la interacción en la navegación es mayor, cuantos más Me Gusta o más reacciones se produzcan por el usuario.

[65] http://tecnologia.elpais.com/tecnologia/2017/05/03/actualidad/1493835469_309268.html.

3.5. Un ejemplo de modelo empresarial: *Facebook* en cifras

Facebook, se configura como un servicio sin coste económico para los usuarios de su red social, pero no nos engañemos, ni ésta ni las otras grandes compañías que operan en el ámbito de Internet son ajenas a la lógica del mercado, no actúan por motivos filantrópicos ni para acercar la tecnología a los ciudadanos sin pretender obtener nada a cambio. *Facebook* es una empresa que cotiza en bolsa, que pone a disposición de sus usuarios una serie de infraestructuras cuyo mantenimiento le comporta ciertos costes y, en consecuencia, tiene como finalidad obtener beneficios económicos.

¿Y cómo lo logra? Sus ingresos los aporta la publicidad pero su activo empresarial lo forman la gran cantidad de datos y metadatos –datos sobre los datos- que almacena en sus servidores y que los usuarios de *Facebook* ceden gratuitamente[66]. El negocio es redondo, sus usuarios donan gratuitamente información de carácter personal (nombre, sexo, localización, dirección de correo electrónico, estado civil, nivel de estudios, hábitos de consumo, preferencias de todo tipo…) que se filtra y clasifica por grupos y se ofrece a anunciantes que la emplearán para el marketing personalizado (el llamado *targeting*[67]). *Facebook*, en la práctica se ha convertido en un software masivo de datos cuyo destino, por el momento, se limita a fines publicitarios.

Mediante este proceder se van configurando perfiles y etiquetas[68] para las personas, que pueden usarse para recibir ofertas de productos y servicios que sean de su interés pero que también puede derivarse en la razón por la que no les concedan un préstamo o un trabajo. Habría que reflexionar también sobre la selección de los hechos relevantes para tal categorización, lo que inevitablemente refleja cierta ideología, así como sesgos y prejuicios.

---

[66] *Facebook* es, de facto, una plataforma dedicada a la creación de perfiles mediante las acciones de sus usuarios, sus deseos, sus preferencias, sus Me Gusta, sus no acciones… transformando toda esta información en datos: en ceros y unos que a menudo reconfiguran nuestra identidad digital. Aunque no se conocen los algoritmos que usa *Facebook* para ello, se han creado herramientas como "What Facebook Thinks You Like" que permiten hacerse una idea de cómo funciona el sistema y como avanza éste según vamos navegando en la web. Disponible para descargar online en https://chrome.google.com/webstore/detail/what-facebook-thinks-you/eoknmaajkanapojcdeccofmeimpddoim. Última consulta 03.06.17.

[67] La publicidad personalizada no es una nueva técnica comercial así como tampoco lo es que los gobiernos espíen a sus ciudadanos, pero el entorno digital contemporáneo amplia dichas posibilidades hasta el infinito, lo que en muchos casos roza la distopía Orwelliana. Este es el caso de las últimas filtraciones llevadas a cabo por WikiLeaks, llamadas "Year Zero" y que ponen de manifiesto las técnicas utilizadas por la CIA para el ciberespionaje entre 2013 y 2016. Según parece no sólo utilizaban las vulnerabilidades técnicas de ciertos aparatos electrónicos estadounidenses y europeos sino que infectaban dispositivos de última generación para acceder a información personal. Así, por ejemplo, mediante malware se consigue acceder a los Smartphones y, entre otros, georastrear al usuario o, mediante las SmartTV, grabar el sonido ambiente, convirtiéndolas en micrófonos y hasta en algunos casos cámaras, encubiertas.

Información disponible para su descarga en https://wikileaks.org/ciav7p1/. Última consulta 05.06.17.

[68] En un reciente artículo del Washington Post, se creó una lista de los 98 datos personales que *Facebook* maneja sobre sus usuarios, sin que éstos sean muchas veces conscientes de ello, y que permiten catalogarlos de muchas y variadas formas. Artículo dispone en https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?utm_term=.079af4e1045f. Última consulta 05.06.17.

Facebook es el gigante de la publicidad comportamental en línea, lo explota y no tiene ningún reparo a la hora de ofrecerse a los anunciantes como mediador entre ellos y los usuarios a cambio de una contraprestación económica. Ha hecho un negocio de ello, presumiendo de poder desglosar a los usuarios de la red social en segmentos potenciales de consumidores según los datos obtenidos por la plataforma: su ubicación, fragmento demográfico, intereses, nivel de conexión o según los Me Gusta[69].

¿Es esto legal? Pues sí. Todo usuario de *Facebook* debe, como requisito para crearse una cuenta, prestar su consentimiento (se presupone que previa lectura) sobre sus términos y condiciones de uso que, si bien consisten en unas cláusulas de adhesión más que abusivas, el usuario parece estar de acuerdo a aceptar cuando crea su perfil. Entonces, ¿dónde está el problema? Dejando de lado la ética empresarial y el mercadeo de nuestra privacidad, el inconveniente principal del almacenamiento masivo de datos es su opacidad. Está demostrado que nuestros datos personales tienen un importante valor de mercado y también que hay empresas dedicadas única y exclusivamente al almacenamiento masivo de datos. Y, si bien hasta ahora se están empleando con fines exclusivamente publicitarios, puede ser que en el futuro no se generen suficientes beneficios y decida emplearse la información personal para otros usos.

Por ejemplo, ¿qué ocurriría si una compañía acumula una deuda impagable y para evitar un concurso de acreedores o una bancarrota, decide vender nuestra información más sensible para generar ingresos? Seguramente las aseguradoras privadas de salud estarían interesadas en saber de antemano el historial médico de aquéllos que solicitan contratar con ellos o, en un escenario peor, son muchos los usos que podrían darse a nuestros datos personales en manos de la economía criminal.

El Big Data en connivencia con Internet, se está convirtiendo en un mercado opaco dónde la materia prima es la vida íntima de las personas, y cuyos ingresos y utilidades son cada día mayores e inversamente proporcionales a la privacidad y a la seguridad jurídica de las personas. Y lo peor, es que aún desconocemos qué aplicaciones futuras tendrá.

De lo que no hay duda es que se está comercializando con nuestros datos personales así como que hay empresas dedicadas -única y exclusivamente- al mercadeo de éstos, sin embargo, dada la falta de transparencia del sector es imposible extraer cifras concretas del negocio de la privacidad.

No obstante, para hacerse una idea aproximada de las ganancias que se generan en torno a ello, basta con examinar la cuenta de resultados de una empresa dedicada a este negocio. Así, siguiendo con el ejemplo de *Facebook*, cuyos últimos resultados presentados son los relativos al último trimestre de 2016, se observa que entre julio y septiembre de 2016, sus ingresos[70] superaron los 7 millones de dólares (unos 6.100 millones de euros), una cifra récord desde el nacimiento de la compañía. Para hacerse una idea de la magnitud de dichas cifras, según el Fondo Monetario Internacional, éstas superarían el Producto Interior Bruto de más de 40 países.

La explicación la conocemos: sus usuarios, cuyo crecimiento parece no tener límites (en la

[69] https://www.facebook.com/business/learn/facebook-ads-choose-audience. Última consulta 05.06.17.

[70] http://www.bbc.com/mundo/noticias-37871331. Última consulta 05.06.17.

actualidad está a punto de alcanzar los 1.800 millones, el equivalente a casi la cuarta parte de la población mundial) y los datos personales de los mismos, vis atractiva de empresas publicitarias que compran espacios en la red social para anunciarse. De hecho, de estos 7 millones de ganancias, 6.820 millones (su 97%) corresponden a ingresos por publicidad. Si dividimos dichos ingresos trimestrales entre los usuarios de la red, *Facebook* habría obtenido un promedio mundial de unos 4 dólares de ganancia por cada uno de sus usuarios, lo que multiplicado por 12, se convierte en 16 dólares anuales. Obviamente estas cifras varían en función del ámbito geográfico (a la cabeza, Estados Unidos y Canadá, mientras que Europa se sitúa ligeramente por encima de la media mundial) y del valor de la oferta y la demanda en cada momento.

Facebook cerró el año 2016 con una media de unos cinco dólares más por cada uno de sus usuarios, con unos ingresos totales de más de 27.500 millones de dólares, un incremento de casi un 650% respecto a los cinco años anteriores dado su incremento constante de usuarios, lo que hace del *targeting* un filón para las empresas anunciadoras cuyo número ha aumentado también exponencialmente[71]. Otra manera de calcular el valor de los datos sería ponerlo en relación con su valor de cotización en bolsa. Siguiendo con *Facebook*, si comparamos su valor bursátil con el número de usuarios de la red social, la cifra resultante es un total de 227 dólares por usuario. Precisamente *Facebook* alcanzó el récord de 375.000 millones de dólares en bolsa, consolidándose como la cuarta empresa más valiosa del Mundo.

Este modelo de negocio gira exclusivamente en torno a la explotación publicitaria de la información de sus usuarios que, paradójicamente, no se ven repercutidos económicamente de ninguna manera. Ante estas cifras, parece lógico preguntarse si no deberían de cobrar a *Facebook* por el uso de sus datos, activo principal de su negocio.

4. Lógica economicista del estándar actual de privacidad

La universalización del mercado ha optado por configurar modelos sociales, económicos y jurídicos únicos que faciliten las relaciones sociales y el libre comercio y las hagan más eficientes, colocando en una posición privilegiada a los regímenes privados frente a los públicos ya que mientras que los primeros pueden dedicarse a buscar su beneficio propio, el Estado tiene la obligación de velar por los intereses de los ciudadanos, desde cierto punto altruista. Este fenómeno se extiende también al ámbito económico y al Derecho[72].

Analizando lo ocurrido con la mercantilización de la privacidad desde un punto de vista económico habría que considerar las normas jurídicas como precios, los precios como costes de oportunidad y el sistema jurídico como al mercado[73]. Así las cosas, las normas jurídicas se instrumentalizan para incentivar o desincentivar a sus destinatarios por lo que se les asignaría un

[71] *Facebook*, junto con *Google*, controla la mitad del mercado de la publicidad en Internet. Estas empresas ven incrementados cada vez más sus ingresos por publicidad online, cuyas cifras han desbancado los medios tradicionales como la televisión que han visto como se retiraban en paralelo los recursos de los anunciantes, seducidos por las nuevas oportunidades de marketing que presenta el Big data.

[72] Véase MERCADO (1994, pp. 127 y ss.).

[73] BERMEO (2016, p. 104).

precio en la ecuación.

Así, siguiendo esta analogía, podemos decir que las normas jurídicas en materia de privacidad se han convertido, quizás sin pretenderlo, en costes de oportunidad positivos en el sentido de que han conseguido incentivar la comercialización de la privacidad con la desregulación del mercado. Ni Internet ni la tecnología son neutrales, son una creación humana y, por lo tanto, responden a la ideología de sus creadores o de los agentes intervinientes que, hasta la fecha, han apostado claramente por almacenar la mayor cantidad posible de datos del mismo modo que han tomado la decisión consciente de vender esa información a terceros, en beneficio propio y en el marco de una decisión empresarial[74].

Estas empresas han adoptado un modelo de negocio en torno a la capitalización de la información personal de sus usuarios en vez de a su protección[75], y lo han hecho en connivencia con los Estados que han resultado cómplices de su actuación.

Si bien es cierto que, al menos en territorio europeo, están explícitamente reconocidos una serie de derechos en torno a la privacidad, en la práctica se ha producido un éxodo masivo de las principales empresas de Internet hacia territorio estadounidense, mucho menos garantista en la materia, tratando de extender el modelo norteamericano más allá de sus fronteras. Estandarizar el derecho, recordemos, cumple con los fines de la globalización.

Esto, en la práctica, supone que empresas como *Google* o *Facebook* están llevando a cabo un tratamiento masivo de datos personales, donde los usuarios firman un cheque en blanco al aceptar los términos y condiciones de uso y resulta verdaderamente difícil seguirles la pista una vez aceptan la política de privacidad. Esta situación escapa a nuestro control y es más que evidente la inseguridad jurídica que sufrimos los ciudadanos, ¿cómo podemos solicitar la cancelación de nuestra información más privada si no sabemos a quién dirigirnos ni siquiera qué saben de nosotros? Pese a tener reconocidos explícitamente en nuestro ordenamiento derechos fundamentales como la intimidad o la protección de datos, éstos se convierten de facto en papel mojado.

Parece ser que tanto usuarios, obligados a pleitear en jurisdicción estadounidense, como gobiernos, que ven como las grandes corporaciones esquivan el cumplimiento de su ordenamiento jurídico, están tomando consciencia de los peligros de comercializar con la información más personal, escenario que ha dado lugar a la creación de un nuevo Reglamento Europeo de Protección de Datos. Esta nueva normativa, que pretende consolidar los estándares de protección a todo el territorio europeo, da un giro en la trayectoria reciente al intentar erradicar estos comportamientos empresariales, convirtiéndose en costes de oportunidad negativos al prever sanciones para supuestos de incumplimiento. Y es que sería deseable que un

[74] DOMÉNECH (2014, pp. 99-133).

[75] No obstante, es cuestionable la eficiencia de este régimen que impone a los usuarios la carga de proteger su privacidad ya que, en Internet, la información sobre un individuo nunca es absolutamente cierta o completa y al no tener el usuario control sobre ésta, no hay manera de corregir hechos erróneos que pueden determinar la decisión de la contraparte, lo que puede llevar a una conducta económicamente ineficiente. También esto aleja a potenciales clientes que por temor a la exposición ilimitada y a la publicidad no deseada, dejan de participar en ciertos comportamientos online.

sistema jurídico pudiera proteger bienes con independencia de su transcendencia económica, pues es indudable que ciertos valores o principios en nuestra sociedad resultan jurídicamente relevantes y son susceptibles de tutela legal con independencia de su eficiencia económica. La privacidad pues, debe empezar a percibirse del mismo modo y pasar a protegerse legislativa y jurisdiccionalmente de una forma real, sin pensar en otros factores economicistas.

No obstante, mucho tendrá que cambiar el *modus operandi* de dichas empresas que solicitan la aceptación de unos términos y condiciones infinitos e indescifrables para contratar la mayoría de los servicios y que no informan con claridad sobre cuál es el destino de nuestros datos personales ni de si éstos cambian de manos. La transparencia debe aumentar necesariamente para hacer efectivos nuestros derechos, pero, así y todo, va a ser muy difícil controlar, por ejemplo, la actividad de los *Data Brokers* que trabajan prácticamente en la clandestinidad.

Además, acuerdos como el *Privacy Shield*, que permite las transferencias transatlánticas de datos personales por "motivos comerciales" eludiendo el tenor literal de la normativa europea, evidencian la visión contrapuesta acerca de la privacidad en los sistemas jurídicos principales y no contribuyen a disipar el escepticismo.

5. Propuestas de futuro: apostar por la privacidad

La privacidad por diseño puede que sea una de las mejores estrategias a seguir a la hora de proteger la intimidad de los ciudadanos que, debido a la configuración por defecto de las páginas web y de sus dispositivos inteligentes resultan cómplices, muchas veces sin saberlo, de prácticas de negocio que menoscaban su privacidad. Los consumidores deben ser capaces de comprender la utilización que de sus datos personales va a hacerse, así como 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.

¿Por qué no se ofrecen servicios fáciles de usar y respetuosos con la privacidad? Sencillamente porque esto sería 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. Pero de ningún modo éstas empresas pueden quedan eximidas en su actividad empresarial de los principios jurídicos fundamentales aplicados en otros ámbitos de la vida cuotidiana, la esfera online de las relaciones sociales y económicas debe de dotarse de seguridad jurídica.

Una forma de proteger a los usuarios de Internet, pasa por aplicar lo que se ha venido llamando *Privacy by design*. Esto implicaría que, por el hecho de navegar por ciertas redes o utilizar determinados servicios de Internet, no se presuponga que los sujetos autorizan la monitorización de su actividad en la red ni otorgan su consentimiento implícito para el almacenamiento y tratamiento de sus datos personales. Ahora viene ocurriendo justo todo lo contrario. Cuando, por ejemplo, nos compramos un nuevo Smartphone, éste viene configurado por defecto para rastrear el mayor número de información posible y así, si no modificamos los parámetros de fábrica, nuestro teléfono nos sorprende diciéndonos cuánto nos queda para llegar a casa después del trabajo, y recordándonos que el próximo fin de semana nos vamos de vacaciones a Benidorm.

Es verdad, sin embargo, que a mucha gente esto le parece de gran ayuda y que se pueden desinstalar estas funciones si no son de nuestro agrado (y si sabemos cómo hacerlo, claro[76]), pero ¿no sería mejor para los usuarios, o al menos no les dotaría de mayor seguridad jurídica, solicitar activamente la prestación de dichos servicios? Al menos de este modo quedaría garantizado la prestación del consentimiento.

La comercialización de estos derechos personalísimos es una cuestión aún no resuelta por el Derecho, siempre el último en llegar. La explotación económica de la privacidad invita como mínimo a reflexionar sobre la verdadera naturaleza de estos derechos más íntimos, dado que su mercantilización es ya una realidad, y de la posible existencia de un derecho de propiedad sobre los mismos[77].

Recientemente, Tim Berners-Lee, inventor de la *World Wide Web*, con motivo del 28 aniversario de su hazaña, reflexionaba[78] sobre el papel actual de Internet y reclamaba una mayor ética en su uso, reivindicando el papel de la Web como un servicio que debe beneficiar a toda la humanidad. En su carta abierta se muestra principalmente preocupado por la pérdida de nuestra información personal en Internet y por la utilización de ésta junto con algoritmos matemáticos para, por ejemplo, hacer campañas políticas capaces de, entre otros, alejar a potenciales votantes de las urnas mediante su redirección hacia sitios de noticias falsas.

La tecnología es una invención humana y como tal, no resulta imparcial. Ésta no funciona de manera autónoma, sino que son las empresas que le dan uso las que dictan su rumbo. El modelo de la publicidad personal por defecto que Internet ha venido adoptando hasta ahora, es fruto de una decisión discrecional orientada únicamente hacia la rentabilidad de dicho medio y no a la protección de los usuarios, pero nada impide reconsiderar el camino recorrido y retroceder en él.

Frente a este panorama, Berners-Lee defiende una transparencia algorítmica que nos ayude a entender cómo se toman las decisiones automatizadas y trabajar con los diversos partícipes del medio para explorar modelos alternativos de negocio en Internet.

6. Reflexiones finales

La innovación tecnológica es admirable y las numerosas ventajas que ha traído con ella merecen reconocerse. No obstante, también ha supuesto ciertos riesgos para algunos derechos

[76] Para personalizar el nivel de privacidad de *Facebook* es necesario hacer click en más de cincuenta botones los cuales requieren elegir entre un total de más de 170 opciones.

Tampoco es fácil borrar una cuenta de usuario de *Facebook*, se permite desactivar las cuentas por lo que, aunque la información no sea pública, esta queda de por vida en la plataforma por si un día el usuario decide retomar su actividad y volver a activar su perfil justo donde lo dejó. Para eliminar definitivamente una cuenta en dicha red social, habría que borrar cada uno de los pasos que se hayan dado en esta plataforma, cada foto, cada comentario, cada Me Gusta… sólo aquellos con tiempo y paciencia suficiente podrán llevar a cabo tan ardua tarea.

[77] Véase BARIÑAS (2013, pp. 1-60).

[78] Disponible en http://webfoundation.org/2017/03/web-turns-28-letter. Última consulta 05.06.17.

fundamentales y cuando, mediante ciertos dispositivos capaces de almacenar y tratar datos personales caprichosamente, se construye un modelo de negocio cuyo propósito no es otro que la obtención de beneficios económicos a costa del quebrantamiento, o al menos del menoscabo de ciertos derechos personalísimos como el derecho a la intimidad, deberíamos poner ciertos límites.

Hay que ser consciente de que durante los últimos años venimos asistiendo a una redefinición de la privacidad, especialmente por el modo en que los particulares exponen su intimidad de forma voluntaria y con ello, el modo de entender la protección de datos ha variado sustancialmente. De hecho, es curioso que el valor de los bienes, tradicionalmente basado en su escasez y en su demanda, haya cambiado radicalmente su lógica en Internet y pase ahora considerarse más valioso cuanto mayor sea el volumen de información que circule por ella, algo explicado hace años por la *Ley de Metcalfe*[79].

No obstante, ello no puede significar una desprotección absoluta de los ciudadanos frente al manejo del Big data, el mercadeo de datos personales debe encontrar sus límites en algún punto. La protección de la privacidad requiere de la intervención de la política pública, no es un sector que pueda dejarse a la autorregulación como se ha estado haciendo hasta ahora pues, en el contexto actual, las pocas corporaciones que controlan Internet operan exclusivamente con finalidad de negocio.

Estas intromisiones en la privacidad pueden dar lugar también a otro tipo de vulneraciones como, por ejemplo, a una discriminación entre los ciudadanos según sean consumidores de bienes básicos o de servicios de pago, estratificando socioeconómicamente a los usuarios.

Bajo el pretexto de la innovación tecnológica no se pueden amparar prácticas abusivas para con ciertos derechos fundamentales que no son ni negociables ni irrenunciables.

Hay que redefinir los límites, el significado y el alcance de los derechos clásicos de intimidad y protección de datos y encontrar un equilibrio que permita el desarrollo tecnológico y la supervivencia de los derechos fundamentales de las personas, dotando de seguridad jurídica a todas las partes implicadas.

El legislador europeo está preocupado por estos temas, como lo demuestra la Propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales [COM(2015) 634 final], incluyendo dentro de su ámbito de aplicación aquellos contratos denominados "gratuitos" en los que el consumidor se obliga a la cesión de determinados datos personales. Con esta regulación, el legislador europeo trata de aunar dos intereses contrapuestos, por un lado, promover el mercado digital mediante el intercambio de datos, por otro lado, proteger los derechos de los consumidores.

Desde el punto de vista de la dogmática jurídica estas nuevas categorías de contratos no encajan bien en la dogmática clásica, que distingue entre contratos gratuitos y onerosos, excluyendo para los primeros los remedios propios de la falta de conformidad de los bienes (del saneamiento).

[79] La Ley de Metcalfe, creada por Robert Metcalfe, cuyo enunciado consiste en "*El valor de una red de comunicaciones aumenta proporcionalmente al cuadrado del número de usuarios del sistema (n2)*", trata de ilustrar cómo el crecimiento exponencial de los usuarios de una red puede aumentar considerablemente su valor, motivo por el cual se utiliza al explicar el valor económico de una tecnología aplicada a las telecomunicaciones.

Aunque tampoco puede decirse que esos contratos sean realmente gratuitos, al tratarse de transacciones en los que el consumidor asume ciertas obligaciones, que tienen un contenido económico. Cuando el consumidor se compromete a ceder sus datos acepta la cesión de la explotación de los mismos al prestador del servicio. Quizá esta cesión aisladamente no reporte a este último un gran beneficio económico, pero unidos estos datos a los de un grupo considerable de usuarios, la situación cambia considerablemente.

Uno de los problemas que puede observarse en este sector de actividad económica es el de la falta de transparencia, ya que muchas veces estos servicios se presentan como "gratuitos", aunque los usuarios son conscientes de que sus datos personales representan una moneda de cambio. Debería quedar claro en las cláusulas del contrato, en la mayoría de los casos predispuestas, cuáles son los compromisos asumidos por el prestador del servicio en consonancia con la normativa sobre protección de datos personales. La doctrina ha defendido que deberían considerarse abusivas aquellas cláusulas en las que el consumidor renuncia a los derechos que le concede la normativa sobre protección de datos personales.

Además, conviene tener presente que este tipo de contratación presenta particularidades específicas, al tener conexión con la protección de los derechos de la personalidad, que son indisponibles en abstracto, pero que, en determinados casos, cabe disponer de ciertos aspectos, como sucede en el caso de la explotación comercial de la imagen de la persona. Precisamente debido a esta particularidad, la posibilidad de poder revocar el consentimiento debería estar siempre presente en este tipo de contratos, aunque suponga, en cierta manera, dejar el cumplimiento del contrato al arbitrio de una de las partes contratantes.

7. Bibliografía

Manuel ALBALADEJO GARCÍA (2013) *Derecho Civil. Introducción y parte general*, t. I, 19ª ed., Edisofer, Madrid.

Désirée BARIÑAS UBIÑAS (2013), "El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. Las nuevas formas de ataque a la vida privada", *Revista Electrónica de Ciencia Penal y Criminología*, n. 15, pp.1-60.

Stephen R. BARNETT (2000), "El derecho a la propia imagen: el right of publicity norteamericano y su correspondencia en el Derecho español", *Revista de Derecho Mercantil*, n. 237, pp. 1225-1250.

Vera BERGELSON (2003), "It's Personal But is it Mine? Toward Property Rights in Personal Information", *UC Davis Law Review*, vol. 37, n. 2, pp. 379-451.

Luis Fernando BERMEO ÁLVAREZ (2016), "Las normas jurídicas: una aproximación desde el convencionalismo jurídico y el análisis económico del derecho", *Inciso*, vol. 18, n. 1, pp. 99-107.

Sergio CÁMARA LAPUENTE (2016), "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).

Ángel CARRASCO PERERA, (2004), *Derecho Civil*, 2ª ed.,Tecnos, Madrid.

Luis Humberto CLAVERÍA GOSÁLBEZ (1984), "Negocios jurídicos de disposición sobre los derechos al honor, a la intimidad y la propia imagen", *Anuario de Derecho Civil*, vol. 37, n. 3, pp. 31-69.

Federico DE CASTRO Y BRAVO (1985), *El negocio jurídico*, Civitas, Madrid.

Miguel DEL FRESNO GARCÍA (2014), "Internet como macromedio: la cohabitación entre los medios sociales y medios profesionales", *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, n. 99, pp. 107-110.

Gabriel DOMÉNECH PASCUAL (2014), "Por qué y cómo hacer análisis económico del Derecho", *Revista de administración pública*, n. 195, pp. 99-133.

Jean DOMAT (1756), *Les Loix Civiles Dans Lew Ordre Naturel, le Droit Public, et Legum Delectus,* 9ª ed., Savoye, Paris.

Amitai ETZIONI (1999), *The limits of privacy*, Basic Books, New York.

M. Paz GARCÍA RUBIO, (2015), "La huella y el legado de Federico de Castro en la moderna protección civil de los derechos de la personalidad", en Díez-Picazo, Luis (dir.), *Glosas sobre Federico de Castro*, Aranzadi, Cizur Menor, pp. 230-277.

Simon GARFINKEL (2000), *Database nation. The death of privacy in the 21st century*, O'Reilly, Sebastopol (EE.UU.).

Inmaculada HIGUERAS (2001), *Valor commercial de la imagen. Aportaciones del right of publicity estadounidense al derecgo a la propia imagen,* Eunsa, Pamplona.

José Luis LACRUZ BERDEJO, Francisco de Asís SANCHO REBULLIDA, Agustín LUNA SERRANO, Jesús DELGADO ECHEVERRIA, (1983), *Elementos de Derecho Civil, Parte General del Derecho Civil*, t. I, v. I,

José Maria Bosch, Barcelona.

Sylwia LINDQVIST (2012), "The concept of transparency in the European Union's residential housing market: A theoretical framework", *International Journal of Law in the Built Environment*, Vol. 4 Issue: 2, pp.99-115.

Marco LOOS (2013), "The Regulation of Digital Content B2C Contracts in CESL", *Amsterdam Law School Research Paper*, n. 10, pp. 611-634.

Ángel LÓPEZ Y LÓPEZ, Vicente Luis MONTÉS PENADÉS, Encarna ROCA TRÍAS, (2003), *Derecho civil, Parte General, Derecho de la Persona*, Tirant lo Blanc, Valencia.

María Rosa LLÁCER MATACÁS (2012), *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, Dykinson, Madrid.

Carlos MARTÍNEZ DE AGUIRRE ALDAZ, Pedro DE PABLO CONTRERAS, Miguel Ángel PÉREZ ÁLVAREZ y María Ángeles PARRA LUCÁN (2015), *Curso de Derecho civil. Derecho privado. Derecho de la persona*, v. I, Colex, 5ª ed., Madrid.

Henri MAZEAUD, Léon MAZEAUD, Jean MAZEAUD, (1974) *Leçons de droit civil*, t.I, 5ª ed., Montchrétien, Paris.

Pedro MERCADO PACHECO (1994), *El análisis económico del derecho: una reconstrucción teórica*, Centro de Estudios Constitucionales, Madrid.

Axel METZGER (2017), "Data as Counter-Performance. What Rights and Duties do Parties Have?", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 8, n. 1, pp. 2-8.

Susana NAVAS NAVARRO (2016), *Mercado digital. Principios y reglas jurídicas*, Tirant lo Blanch, València.

Xavier O 'CALLAGHAN MUÑOZ, Mª. Begoña FERNÁNDEZ GONZÁLEZ (2017), *Compendio de Derecho Civil Tomo I: Parte general*, Editorial Centro de estudios Ramón Areces, Madrid.

Robert Joseph POTHIER (1825), *Traité des Obligations*, en M. Dupin, *Oeuvres de Pothier, contenant les traités du Droit français*, 9ª ed., Béchet aîné, Paris.

Samuel PUFENDORF (1672), *De jure naturae et gentium libri octo*, Londini Scanorum, Londres.

Oliver RADLEY-GARDNER y Hugh BEALE (2016), *Fundamental Text son European Private Law*, Bloomsbury, Inglaterra.

Daniel J. SOLOVE (2006), "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, vol. 154, n. 13, pp. 477-560.

Gerald SPINDLER (2016), "Contratos de suministro de contenidos digitales: ámbito de aplicación y visión general de la Propuesta de Directiva de 9.12.2015", *InDret 3/2016*, (http://www.indret.com/pdf/1243.pdf).

Andrea TORRENTE, Piero SCHLESINGER, (2009) *Manuale di diritto privato*, 19ª ed., Giuffrè, Milán.

Antonio TRONCOSO REIGADA (2010), *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, València.

Samuel WARREN y Louis BRANDEIS (1995), *El derecho a la intimidad,* Benigno PENDÁS y Pilar BASELGA (traductores), Cuadernos Civitas, Madrid.

Christiane WENDEHORST (2016), "Consumer Contracts and the Internet of Things", en Reiner SCHULZE y Dirk STAUDENMAYER (editores), *Digital Revolution: Challenges for Contract Law in Practice*, Hart Publishing, Inglaterra, pp. 189-223.

8. Tabla de jurisprudencia citada

Tribunal, Sala y Fecha	*Ar.*	*Magistrado Ponente*	*Partes*
Ohio Court of Appeal	341 N.E.2d 337/1975	J. Fink	Shibley c. "Time, Inc.".
STC, 1ª, 25.04.1994	RJ 117	José Gabaldón López	D. Ana G.O. c. "Editorial Origen, S.A.".
Apellate Court of Illinois	652 N.E.2d 1351/1995	Edward C. Hofert	Patrick E. Dwyer c. American Express Company
Virginia Supreme Court	95-7479/1996	William T. Newman	Avrahami c. "U.S. News & Worls report".
STC, 4ª, 30.11.2000	291/2000	Julio Diego González Campos	Defensor del Pueblo, contra los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
STC, 2ª, 26.03.2001	81/2001	Carles Viver Pi-Sunyer	Emilio Aragón Álvarez c. "Proborín, S.L.".
STC, 1ª, 18.06.2001	139/2001	Pablo Manuel Cachón Villar	Alberto Cortina de Alcocer c. "Diez Minutos".
STC, 1ª, 22.04.2002	82/2002	Pablo García Manzano	Manuel Ruiz Claros y Francisco Vivas Andrades c. AP Málaga.
STC, 2ª, 28.01.2003	14/2003	Vicente Conde Martín de Hijas	Mederico Serna Vergara c. AN.
New Hampshire Supreme Court	816 A.2d/2003	Paul Barbadoro	Remsbourg c. "Docusearch, Inc.".
STS, 1ª, 19.07.2004	RJ 5462	José Ramón Ferrándiz Gabriel	Romulo Gonzalvo Boix c. "Ediciones Zeta, S.A. y D. Bartolomé".
STC, 1ª, 16.04.2007	72/2007	Manuel Aragón Reyes	María escudero Cuenca c. "Diario 16".
STS, 1ª, 18.06.2012	RJ 4183	Jose Antonio Seijas Quintana	Matías c. Gregoria y Eulalio.
SSTJUE 21.03.2013	C-92/11	M. Safjan	"RWE Verttrieb AG" c. "Verbraucherzentrale Nordrhein-Westfalen eV".
STS, 1ª, 9.05.2013	RJ 1916	Rafael Gimeno-Bayon Cobos	"Ausbanc Consumo" c. "BBVA, S.A."y "NCG banco S.A.U.".
SSTJUE 30.04.2014	C-26/13	A. Prechal	Árpad Kásler y Hajnalka Káslerné Rábai y "OTP Jelzálogbank Zrt".

STS, 1ª, 8.09.2014	RJ 3903	Francisco Javier Orduña Moreno	Varios c. Caja Segovia.
SSTJUE 26.02.2015	C-143/13	A. Prechal	Bogdan Matei y Ioana Ofelia Matei c. "SC Volksbank Romania S.A.".
STS, 1ª, 24.03.2015	RJ 1279	Rafael Saraza Jimena	Ausbanc Consumo c. "Caja de Ahorros y Monte de Piedad de Córdoba, Caja Sur".
STS, 1ª, 25.03.2015	RJ 1280	Eduardo Baena Ruiz	Jon y Tamara c. "BBVA, S.A.".
SSTJUE 16.10.2015	C-362/14	T. von Danwitz	Maximillian Schrems c. Data Protection Commissioner.
SAN, 4ª, 29.03.2017	RJ 514	Juan Francisco Martel Rivero	Ministerio Fiscal c. Olegario