DESDE LA PROTECCIÓN DE DATOS DE LOS CONSUMIDORES A LAS ORGANIZACIONES COMO CONSUMIDORES DE DATOS PERSONALES

FROM CONSUMER DATA PROTECTION TO ORGANIZATIONS AS CONSUMERS OF PERSONAL DATA

Actualidad Jurídica Iberoamericana Nº 16, febrero 2022, ISSN: 2386-4567, pp. 690-713

Raquel PÉREZ DÍAZ

ARTÍCULO RECIBIDO: 15 de noviembre de 2021
ARTÍCULO APROBADO: 10 de enero de 2022

RESUMEN: Desde sus orígenes el derecho a la protección de datos de carácter personal y su regulación han pretendido paliar la incidencia negativa que para la privacidad conllevaban los avances tecnológicos; comprobándose, actualmente, que junto al objetivo de que los interesados (titulares de los datos personales) mantengan el control sobre sus datos, debe prestarse especial atención y fijarse como objetivo evitar que el uso de los datos personales pueda conllevar un control sobre los interesados, al descubrirse la potencialidad de los datos para el logro de objetivos y mejora de los resultados de negocio.

PALABRAS CLAVE: Protección de datos, datos personales, consumidores, comercio electrónico, contratación online, transparencia, consentimiento.

ABSTRACT: *From its origins the right to the protection of personal data and its regulation have tried to alleviate the negative impact that technological advances entailed for privacy; verifying, currently, that together with the objective that the interested parties (holders of personal data) maintain control over their data, special attention must be paid and the objective should be to avoid that the use of personal data may lead to control over the interested parties, when discovering the potential of the data to achieve objectives and improve business results.*

KEY WORDS: *Data protection, personal data, consumers, electronic commerce, online contracting, transparency, consent.*

I.- INTRODUCCIÓN

El imparable crecimiento del consumo en el mercado digital, tanto de productos y servicios que podríamos considerar "tradicionales" como de los nuevos productos, servicios y contenidos digitales que surgen a partir del desarrollo tecnológico, genera importantes desafíos en diferentes ámbitos jurídicos y entre ellos, destacamos aquellos vinculados a la protección de datos de carácter personal, pues el mundo digital no solo no es ajeno a la privacidad, sino que impacta directamente sobre ella, de una forma inalcanzable para el mercado tradicional u offline. Tanto es así, que teniendo en cuenta un escenario en el que la globalización y el desarrollo tecnológico propiciaron una recogida e intercambio de datos sin precedentes, el legislador comunitario se ha visto obligado en la necesidad de afrontar dicho desafío a través del Reglamento General de Protección de Datos (UE) 2016/679 679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante Reglamento General de Protección de datos o RGPD), a fin de mitigar la preocupante pérdida del control que sobre sus datos personales poseen los interesados en el mundo digital y, la consiguiente, merma del derecho a la protección de datos y de otros derechos fundamentales estrechamente vinculados a éste, como son: en primer término, los derechos al honor, a la propia imagen y a la intimidad personal y familiar, y, en segunda instancia, los derechos a la igualdad, no discriminación y libertad personal.

Partiendo del marco normativo básico de referencia – Reglamento (UE) 2016/679, Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (LOPDGDD) y Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI)–, inicialmente, se abordarán los requerimientos previstos en la normativa de protección de datos para llevar a cabo las operaciones de procesamiento de datos personales derivadas de las contrataciones de bienes y servicios online, haciendo hincapié en como los principios rectores del tratamiento contribuyen

• Raquel Pérez Díaz
Profesora Ayudante Doctora. Área de Derecho Civil.
Universidad de Oviedo
perezdraquel@uniovi.es

en el logro del objetivo que se marcó el legislador europeo de devolver a los interesados el control sobre sus datos personales. En base a los requerimientos normativos, se analizarán las deficiencias que, frecuentemente, se localizan en las plataformas y tiendas online en lo que se refiere a transparencia y legitimación del tratamiento; ya sea desde las carencias en el cumplimiento del principio de transparencia tanto a nivel de contenido como a nivel de comprensión del alcance que conlleva la aceptación de las políticas de privacidad, la captación excesiva de datos, el desequilibrio de las partes intervinientes, hasta los supuestos en los que esos fallos en la presentación de la preceptiva información o en la debida proporcionalidad pueden derivar en problemas de licitud para el tratamiento.

Continuaremos planteando la problemática que podría conllevar el condicionamiento al que se ve sometido el consumidor, ya que, a partir de la aplicación de las tecnologías emergentes sobre su información personal junto a técnicas de marketing y prospección comercial, podría ponerse en entredicho la libertad de elección del consumidor, siendo evidente muestra de ello las cada vez más frecuentes secciones de "recomendaciones" o similares. Conocer las capacidades de procesamiento de datos de tecnologías como big data, apta para crear una serie a medida de las tendencias o gustos que han mostrado los consumidores, nos lleva a preguntarnos si, realmente, consumimos lo que necesitamos y/ o queremos o si consumimos lo que quieren vendernos y nos hacen pensar que necesitamos y/o queremos, colocando ante nosotros el producto, servicio o contenido, induciéndonos a adquirirlo aunque no lo necesitemos.

Por último, debemos tener en cuenta que el comercio electrónico y sus implicaciones en materia de protección de datos no finalizan con el cumplimiento por las organizaciones de los principios y obligaciones establecidos en la normativa de aplicación, pues los datos personales se han convertido en un activo de gran valor, muy codiciado por una gran mayoría de las entidades, ya que su análisis puede reportarles importantes beneficios, convirtiéndose en objeto de comercio y mercantilización. Así, encontraremos un gran número de bienes, servicios y contenidos que pueden obtenerse por los consumidores sin contraprestación económica, pagándose en datos[1] que, llegado el momento, serán objeto de aprovechamiento para colocarante nosotros el siguiente producto de su campaña. La nueva normativa de protección de datos, sin duda, ha proporcionado respuesta a parte de los retos que inspiraron su aprobación, pero en apenas tres años desde su plena aplicación ha mostrado importantes lagunas para hacer frente a las capacidades y aplicaciones de las nuevas tecnologías y al creciente valor de los datos personales, por lo que se analizarán sus implicaciones con la normativa de

1 Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.
Real Decreto-ley 1/2021, de 19 de enero, de protección de los consumidores y usuarios frente a situaciones de vulnerabilidad social y económica

protección al consumidor y las problemáticas para las que las citadas normativas no han abordado o, bien, no han proporcionado respuestas legales plenamente satisfactorias.

II.- EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Sin ahondar en el origen y evolución del derecho a la protección de datos, pues no es el objeto del presente trabajo, simplemente indicar que desde sus orígenes ha pretendido responder a la interferencia que la tecnología supone para la privacidad, desde la fotografía instantánea[2] hasta el reto actual que supone la inteligencia artificial y otras tecnologías o usos disruptivos. Así, el derecho a la protección de datos de carácter personal se ha construido en los ordenamientos jurídicos europeos a partir derecho a la autodeterminación informática, concepto cuyo origen podemos encontrar en el Tribunal Constitucional alemán; y que se reitera en nuestra Constitución Española (CE) en su artículo 18 apartado 4 "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", consolidando la independencia del derecho a la protección dedatos personales de otros derechos fundamentales como el derecho a la intimidad y a lapropia imagen, con los que guarda una estrecha relación[3]; y, configurándose, conforme al criterio expresado en la Sentencia del Tribunal Constitucional (STC) 94/1998, de 4 de mayo[4] (en línea con el concepto que continúa reflejándose en la normativa de referencia), como el derecho de los titulares de los datos a controlar el uso que se hace de los mismos[5], y, precisamente, al efecto y con el espíritu de devolver a los interesados (o titulares de los datos personales) el control sobre sus datos personales, tras detectarse la insuficiencia del marco normativo del momento ante un escenario de recogida, procesamiento e intercambio masivo y sin precedentes propiciado por las nuevas tecnologías y los nuevos usos de las tecnologías preexistentes, se

2 En 1890 los jueces norteamericanos Samuel Warren y Louis Brandeis recogen la primera mención al derecho a la protección de datos de carácter personal, en su artículo "The Right to Privacy", mostrando su preocupación por la invasión en la privacidad que se derivaba de ciertos avances tecnológicos como la fotografía, pero, especialmente, por el alcance de la prensa y los límites que, según entendían estaba sobrepasando.

3 STC 292/2000, de 30 noviembre (RTC 2000, 292): "Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18 apartado 1 CE con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establece la Ley." (…) "De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual." (…)

4 Primera referencia en la jurisprudencia española al derecho fundamental a la protección de datos de carácter personal.

5 Ibidem: "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona a decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quien posee esos datos personales y para qué." (…)

aprueba el Reglamento Europeo de Protección de Datos[6], y, por consiguiente, y en cumplimiento del mandato del legislador comunitario, se procede a la adecuación de ordenamiento jurídico nacional, a través de la aprobación de la Ley Orgánica 3/2018.

Previamente a entrar a analizar determinados aspectos de la nueva normativa de protección de datos y su repercusión, implicaciones y problemáticas en el ámbito del consumidor, conviene clarificar el concepto de dato de carácter personal, y, especialmente, mostrar su alcance a nivel práctico. Según las definiciones proporcionadas por el artículo (art.) 4.1 RGPD, se entiende por dato personal "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". Con ello, y a sensu contrario, se puede concluir que todos aquellos datos que se encuentren disociados no se consideran personales, y en este caso, no se aplicará la regulación de protección de datos dado que se trata de datos pertenecientes a una persona que no se puede identificar.

Respecto al alcance del concepto de dato personal, resulta de gran utilidad para su comprensión detenerse en dos puntos:

- En primer lugar, debe tenerse en cuenta que la normativa incluye en el concepto de dato personal aquellas informaciones que, incluso, indirectamente, puedan conllevar la identificación del interesado, precisándose dicho proceso de identificación indirecta en las orientaciones proporcionadas por el Grupo de Trabajo del artículo 29 al señalar "el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. (…) Incluso una información auxiliar, como, por ejemplo, "el hombre que lleva un traje negro", puede identificar a alguno de los transeúntes que esperan en un semáforo"[7].

6 Considerando 6 RGPD: "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales han aumentado de manera significativa (…)".
Considerando 7 RGPD: "(…) las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas".

7 Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio, por el Grupo de Trabajo del artículo 29 (01248/07/ES, WP 136).

- En segundo lugar, debemos conocer la amplitud real del concepto "dato personal", pues más allá de las informaciones identificativas obvias como son el nombre y apellidos, el DNI u otros identificadores únicos (imagen, huella dactilar, dirección IP, entre otros), se engloban múltiples informaciones relativas al interesado, como es el caso de los datos relativos al consumo energético[8], concretamente, los datos relativos a la curva de carga horaria asociados al CUPS (código universal de puntos de suministro); conclusión que, incluso con una mayor amplitud, se extendería a los datos de consumo en el comercio electrónico (tiendas online), de las plataformas online (servicios streaming) o del uso de determinadas tecnologías (aplicaciones corporativas vinculadas a pulseras de actividad)m pues no solo nos proporcionará información relativa al momento de uso, sino también información relativa a los gustos y preferencias del consumidor, poder adquisitivo, hábitos de consumo o, entre otros, quizás incluso hasta información relativa al estado de salud del interesado.

Para concluir, debe tenerse en cuenta con el concepto de "dato personal", que si bien en el nuevo marco legal desaparecen los antiguos niveles de seguridad de los datos, actualmente se establecen ciertas garantías añadidas para los llamados datos de categorías especiales[9] ("datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física"), a los que, en cierto modo, se asemejan los datos relativos a condenas e infracciones penales.

III.- PRINCIPALES PROBLEMÁTICAS Y DEFICIENCIAS DETECTADAS EN PLATAFORMAS YTIENDAS ONLINE

Definido el concepto y alcance de "dato personal" y, por consiguiente, el objeto de protección de la normativa vigente, se analizarán las principales implicaciones y problemáticas que se derivan para el comercio electrónico de la aplicación de la normativa de protección de datos de carácter personal.

a.- Respecto a los principios rectores del tratamiento:

8 STS, Sala de lo Contencioso-administrativo, Sección 3ª, 12 Jul. 2019, (ECLI:ES:TS:2019:2484), FJ 3: "Los datos de consumo de energía eléctrica individualizados y con desglose horario, permiten a quien tenga acceso a esa información y la vincule con la identidad del titular del contrato de suministro, conocer los hábitos de conducta privados de dicho consumidor, tales como las horas ordinarias de entrada y salida del domicilio, la hora en la que se va a dormir, las zonas horarias en las que más actividad en la vivienda o en el local de negocio, el nivel de electrificación, la utilización de aparatos de refrigeración o calefacción, incluso si vive solo/a o no, entre otros. En definitiva, proporciona una información objetiva que afecta a la esfera privada de cada consumidor y que puede proporcionar unas pautas de comportamiento diario de una persona".

9 Art. 9 apartado 1 RGPD.

El Reglamento (UE) 2016/679, en su art. 5[10], recoge los principios aplicables a toda actividad que conlleve el procesamiento de datos personales, y que pueden concretarse en los siguientes puntos:

- Principios de licitud, lealtad y transparencia: Tratar los datos de forma leal, lícita y transparente, esto es, encontrándose el interesado informado de los términos y condiciones en los que se producirá el tratamiento de sus datos, ajustándose dicho tratamiento a la expectativa razonable del interesado en base a la información proporcionada y al amparo de alguna de alguna de las bases de legitimación determinadas por la propia normativa (y, en su caso, bajo alguna de las excepciones a la prohibición general de tratamiento de categorías especiales de datos personales).

- Principio de limitación de la finalidad: Recoger los datos bajo una finalidad determinada, quedando, a priori, restringido su uso para otras finalidades diferentes de la finalidad original para la cual fueron recabados.

- Principio de exactitud: Ejecutar el tratamiento sobre datos personales veraces o exactos y actualizados.

- Principio de minimización: Ajustar la recogida y el posterior tratamiento de datos personales a aquellas informaciones que resulten imprescindibles para atender a la finalidad a la que servirán.

- Principio de limitación del plazo de conservación: Limitar la conservación de los datos personales al plazo estrictamente necesario para las finalidades del tratamiento.

10 Art.5 RGPD: "1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

- Principios de integridad y confidencialidad: Garantizar la seguridad de los datos y preservarlos de accesos indebidos o no autorizados.

- Y, por último, principio de responsabilidad proactiva: Tener la capacidad de demostrar que se está cumpliendo con los requerimientos establecidos por la normativa.

En el ámbito del consumo online, el cumplimiento de esos principios, al menos, en toda su extensión, plantea ciertos problemas, pues no siempre se respeta el mandato del legislador. ¿Conoce el interesado el uso que se está haciendo de sus datos? ¿Conoce el interesado la existencia de un tratamiento que afecta a sus datos personales? ¿Conoce para que se van a utilizar sus datos personales? ¿Se restringe el uso de los datos a la gestión y ejecución de la transacción comercial? ¿Únicamente se recogen aquellos datos imprescindibles para llevar a cabo la prestación del servicio? ¿Es consciente del valor que tienen sus datos personales?

La Agencia Española de Protección de Datos (AEPD) ha tenido ocasión de pronunciarse en diferentes ocasiones sobre las deficiencias que se presentan en el consumo de contenidos y en la contratación electrónica[11] [12], siendo posible resaltar las siguientes deficiencias:

A nivel de transparencia, partiendo del contenido exigido por la normativa vigente, concretamente, en los arts. 13 y 14 del RGPD, prácticamente todos los puntos plantean carencias en la práctica.

Conforme a lo establecido en el citado art. 13, cuando los datos son obtenidos directamente del propio interesado, se facilitará la siguiente información, a fin de que éste conozca los términos en los que se desarrollará el tratamiento de sus datos personales:

- Identidad y datos de contacto del responsable de tratamiento y, en su caso, de su representante.

- Datos de contacto del delegado de protección de datos.

- Fines del tratamiento y base jurídica del tratamiento.

- En su caso, los intereses legítimos del responsable o de un tercero sobre los que pretende sustentarse el tratamiento de los datos personales.

11 De forma más reciente, a partir del Plan de Inspección de Oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadoras de energía.

12 Informe sobre políticas de privacidad en internet, adaptación al RGPD, publicado por la Agencia Española de Protección de Datos en septiembre de 2018.

- Destinatarios o categorías de destinatarios.

- Intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en su caso, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de éstas o al lugar en que se hayan puesto a disposición.

- Periodo de retención o plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

- Derechos legales del interesado en materia de protección de datos.

- En su caso, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

- Derecho a presentar una reclamación ante una autoridad de control.

- Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos.

- Existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

En aquellos casos en los que los datos no son obtenidos del propio interesado, además de la información anterior, se informará al interesado sobre los siguientes extremos:

- Categorías de datos personales de que se trate.

- Fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

El problema no radica únicamente en las carencias sobre en el contenido exigido por la normativa (colocándose a la cabeza la falta de mención sobre los destinatarios de los datos, así como la referencia a los plazos durante los cuales los datos serán objeto de tratamiento y conservación por el Responsable de Tratamiento; lo que, a su vez, deriva en un incumplimiento o cumplimiento

deficiente del principio de limitación del plazo de conservación), sino también sobre la forma de presentación de dicha información, en ocasiones, oscura e incomprensible para el usuario medio, o de forma vacía o excesivamente genérica, maquillando los textos a fin de dar una apariencia de legalidad; no permitiendo, ya sea de una u otra forma, conocer al interesado la extensión y condiciones del tratamiento.

A fin de evitar la llamada fatiga informativa, el antiguo Grupo de Trabajo del artículo 29 (GT 29), en sus Directrices sobre transparencia, recomienda que en el contexto online se presente la información a los usuarios en diferentes capas[13], al igual que se recoge en la LOPDGDD[14].

En ocasiones, podría incluso plantearse la situación de que el interesado tan siquiera conozca la existencia del tratamiento (como, por ejemplo, ocurre con la monitorización que se realiza a través de las cookies), ya sea porque no todas las finalidades aparecen correctamente identificadas en la política de privacidad o, directamente, porque se desarrollan en segunda instancia, reutilizándose los datos para otras finalidades diferentes de la/ original/ es, teniendo algunas de ellas una gran repercusión para el interesado, como sucede en el caso de tratamientos que impliquen decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente al interesado, elaboración de perfiles o la aplicación de técnicas de scoring. Asimismo, deben tenerse en cuenta los supuestos en los que las organizaciones emplean técnicas para el enriquecimiento de los datos de sus sistemas mediante la combinación de diferentes fuentes de información, como ejemplifica la AEPD con la Base de Datos de Consumidores y Puntos de

13 Directrices sobre la transparencia en virtud del RGPD del Grupo de Trabajo del artículo 29, adoptadas el 29 de noviembre de 2017, revisadas por última vez y adoptadas el 11 de abril de 2018: "En concreto, el GT29 recomienda que se utilicen declaraciones/avisos de privacidad estructurados en niveles para enlazar con las distintas categorías de información que se debe facilitar al interesado, en lugar de mostrar toda esta información en un solo aviso en pantalla, a fin de evitar la fatiga informativa. Las declaraciones/ avisos de privacidad estructurados en niveles pueden ayudar a resolver la tensión entre la integridad y la comprensión, en particular al permitir que los usuarios naveguen directamente a la sección de la declaración/aviso que desean leer".

14 Art. 11 de la LOPGDD: "1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. 2. La información básica a la que se refiere el apartado anterior deberá contener, al menos: a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento. c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a22 del Reglamento (UE) 2016/679. Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679. 3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también: a) Las categorías de datos objeto de tratamiento. b) Las fuentes de las que procedieran los datos".

Suministro (Base de Datos creada de acuerdo con lo establecido en el art. 7 del Real Decreto 1435/2002, de 27 de diciembre) y proveedores externos de repertorios telefónicos.

Otro problema recurrente, se deriva de la recogida innecesaria de datos personales, tanto en aquellos casos en los que se captan, directamente, del interesado, como en aquellos en los que se obtienen a partir de otras fuentes, y, en este caso a su vez, se plantean problemas, tanto para quien recaba datos que pudieran considerarse excesivos a fin de personalizar la oferta para el interesado, como de las entidades que recaban datos innecesarios y que no se emplearán en sus procesos de negocio.

Respecto a los plazos de conservación, el problema detectado por la AEPD, no se agota con la ausencia o deficiencia de la debida información sobre los plazos de conservación o "criterios utilizados para determinar este plazo" en las políticas de privacidad, sino que se extiende a la aplicación efectiva del principio de conservación, pues las entidades carecen de políticas de retención y, aún contando con calendarios de conservación definidos, no los ejecutan. Asimismo, se presenta habitualmente la situación de que las entidades, en aquellos casos en los que amparan el tratamiento en el consentimiento del interesado, no bloquearan ni suprimirán los datos personales hasta que medie una petición por parte del interesado; no siendo ésta una práctica muy recomendable, aconsejándose por parte de la propia agencia que se realicen expurgos una vez haya transcurrido "un periodo de tiempo razonable" o "se implanten procedimientos de revisión periódica".

En el ámbito de la contratación online, nos encontramos ante una particularidad que complica la problemática legal, especialmente, en el ámbito de protección de datos de carácter personal, hablamos de la difuminación de las fronteras físicas y la consiguiente convergencia de diferentes ordenamientos jurídicos. Así, al margen del desconocimiento que pueda presentarse en los titulares de los datos, a nivel de las posibles transferencias internacionales[15] que se lleven a cabo sobre sus datos personales y, especialmente, de la repercusión que conlleva la ejecución de tratamientos transfronterizos en los que participan países sin un nivel de protección adecuado; e incluso, quizás, en algunas ocasiones, derivado de la pérdida de control sobre la cadena de suministro, un desconocimiento por parte de los propios responsables de tratamiento de la existencia de dichas transferencias internacionales; actualmente, nos encontramos con el problema añadido de la incertidumbre jurídica que genera que el marco del Escudo de Privacidad entre la

15 Tal como indica la AEPD: Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Unión Europea – Estados Unidad y Suiza haya quedado invalidado[16], el hecho de que se esté cuestionando la validez de las cláusulas contractuales tipo (opción hacia la que recurrieron la mayor parte de las organizaciones que se vieron afectadas por la anulación del Privacy Shield) y la sombra de que bajo la prerrogativa de la seguridad nacional, el Gobierno de Estados Unidos podrá acceder a la información albergada por todas las empresas norteamericanas con independencia de la localización de sus servidores[17].

De todos los supuestos anteriormente expuestos podrían derivarse graves problemas para la licitud del tratamiento, muy especialmente, en aquellos casos en los que el tratamiento pretenda sustentarse sobre el consentimiento del interesado, pues no debemos olvidar que dicho consentimiento deberá ser, en todo caso, informado. Conscientes de la problemática existente, la AEPD ha publicado, en septiembre de 2018, el "Decálogo para la adaptación al RGPD de las políticas de privacidad en Internet", de gran utilidad para una correcta elaboración (o, en su caso, adaptación a la normativa vigente) de las Políticas de Privacidad online.

Para finalizar, las referencias al cumplimiento de los principios rectores, deberá hacerse mención a la problemática que puede suponer en la contratación online ofrecer garantías sobre la identificación del interesado contratante, a fin de evitar supuestos de repudio e, incluso, suplantaciones de identidad (problema que persiste en los procesos posteriores a la contratación); la AGPD ha detectado una creciente inquietud en las organizaciones sobre la identificación del contratante y las soluciones técnicas para evitar suplantaciones de identidad, poniéndose sobre la mesa la utilización de tecnologías de reconocimiento facial y la firma manuscrita electrónica[18] y sus implicaciones legales, pues introduciría la utilización

16 Sentencia del Tribunal de Justicia de la Unión Europea, 16 de julio de 2020 (Asunto C-311/18), por la que se anula la Decisión 2016/1259 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad (Privacy Shield) para las transferencias internacionales de datos a EEUU.

17 Ley de Aclaración del Uso Legal de Datos en el Extranjero (CLOUD Act) "Este proyecto de ley enmienda el código penal federal para especificar que un proveedor de servicios de comunicaciones electrónicas (ECS) o servicios informáticos remotos (RCS) debe cumplir con los requisitos existentes para preservar, respaldar o divulgar el contenido de una comunicación electrónica o registros de no contenido o información perteneciente a un cliente o suscriptor, independientemente de si la comunicación o el registro se encuentran dentro o fuera de los Estados Unidos" (Aclaración de la Ley de Uso Legal de Datos en el Extranjero o la Ley CLOUD - https://www.congress.gov/bill/115th-congress/house-bill/4943).

18 Ley 59/2003, de 19 de diciembre, de firma electrónica: "La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control".

de datos biométricos[19][20]. Así como el reto que conlleva asegurar la integridad de los documentos de contratación y la acreditación de ésta en sí misma.

b.-Respecto a las bases de legitimación del tratamiento:

Conforme a lo establecido en el art. 6 RGPD "el tratamiento solo será lícito si se cumple, al menos, una de las siguientes condiciones":

- Consentimiento del interesado.
- Necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
- Necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
- Necesario para proteger intereses vitales del interesado o de otra persona física.
- Necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- Necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

De la lectura del citado precepto, se descarta la aplicación al ámbito del comercio electrónico de ciertas bases de legitimación (interés vital y cumplimiento de una misión realizada en interés público o en el ejercicio de poderes *públicos* conferidos al responsable); entendiéndose que, en principio, el tratamiento de datos personales derivado de la transacción comercial se ejecutará al amparo de

19 Art. 4 apartado 14 RGPD: "Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

20 Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía de la AGPD - Recomendaciones: "Es importante que se utilicen sistemas con garantías adicionales del estilo de lo definido en el en la normativa del PSD2: autenticación reforzada del cliente (basada en la utilización de dos o más elementos categorizados como conocimiento -algo que solo conoce el usuario-, posesión -algo que solo posee el usuario– e inherencia - algo que es el usuario- (…) Puede interpretarse que de acuerdo con el art. 4 del RGPD el concepto de dato biométrico incluiría la identificación y la verificación/autenticación (verificación uno contra uno, verificación uno contra varios). Sin embargo y, con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biometría (uno a varios) y no en el caso de verificación/autenticación biométrica (uno a uno). No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos (…)".

la ejecución de un contrato o, en su caso, del cumplimiento de las obligaciones del Responsable del Tratamiento, por ejemplo, en materia contable, fiscal o de prevención del blanqueo de capitales y la financiación del terrorismo, entre otras. Pero, ¿Realmente se agotan las actividades de tratamiento con la transacción comercial? Es más, ¿Empieza el tratamiento de datos personales a partir de la petición de servicio o se han procesado datos con anterioridad?

En aquellos casos en los que los usos previstos de los datos personales vayan a exceder de la ejecución del contrato, la prestación del servicio contratado y del cumplimiento de las obligaciones legales, se precisará del sustento legal de otras bases de legitimación, como el interés legítimo del Responsable de Tratamiento (o, incluso, de un tercero) o el consentimiento del interesado.

Habida cuenta de que los problemas que pudieran derivarse del interés legítimo como base legal para el tratamiento, en esencia, no difieren demasiado de la problemática que pudiera presentar en el comercio offline, es decir, desequilibrio de intereses con prevalencia de los derechos de los interesados sobre el interés alegado por el Responsable de Tratamiento; merece la pena detenerse sobre el consentimiento del interesado como base de legitimación del tratamiento y, concretamente, sobre su adecuación a las premisas establecidas por el RGPD[21], esto es: libre, específico, informado e inequívoco; detectándose deficiencias en todas y cada una de las premisas mencionadas[22].

- En primer lugar, se plantean ciertas dudas sobre la libertad de otorgamiento del consentimiento del interesado[23], pues, en ocasiones, se aprecia cierto desequilibrio entre las partes al no poder apreciarse/ valorarse por el usuario el alto precio que está pagando por el uso de ciertos servicios o el acceso a ciertos contenidos digitales; a lo que debe añadirse un cada vez más generalizado "permiso inconsciente" del usuario[24], como sucede en el caso de los banners habilitados para la aceptación de las políticas de cookies.

21 Art. 4 apartado 11 RGPD "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

22 Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 4 de mayo de 2020 por el Comité Europeo de Protección de Datos.

23 Quedando aún pendiente determinar la incidencia que tendrá en el ámbito de la protección de datos y de sus clausulados "la lucha librada durante las últimas épocas por aflorar las cláusulas abusivas y lograr su supresión de los contratos (...)". La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y a nueva Directiva de suministro de contenidos digitales). De Barrón Arniches, P.: "La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)", Cuadernos Europeos de Deusto, núm. 61, 2019, p.59.

24 Ibidem, p.56.

- Respecto al carácter específico que debe predicarse del consentimiento, la normativa exige cierta granularidad, es decir, otorgar al usuario la posibilidad de aceptar el tratamiento de forma selectiva e independiente para cada una de las finalidades y rehusar de la típica formula genérica "he leído y acepto el tratamiento de mis datos personales".

- Sin entrar a analizar cada uno de los aspectos esenciales[25] que requieren para hablar de consentimiento informado, es posible concluir que las carencias señaladas a nivel de transparencia en el apartado anterior nos conducen al incumplimiento de la tercera premisa.

- Por último, quedaría pendiente valorarse el carácter inequívoco del consentimiento (entendido como acción afirmativa), tratándose con toda probabilidad de uno de los principales desafíos para la adecuación a la normativa de los medios de obtención del consentimiento en el entorno online, pues el uso de casillas premarcadas, la redacción de los clausulados presuponiendo la aceptación y requiriendo de una acción para desistir u oponerse al tratamiento, las deficiencias en la identificación de las acciones de las que se desprenderá la aceptación o el uso del consentimiento diferido[26], continúan lastrando el cumplimiento de la normativa de protección de datos en el mundo digital.

Al igual que ocurría en el caso de la presentación de la debida información a través de las Políticas de Privacidad, el Responsable de Tratamiento debe prestar especial atención al diseño y a la forma en la que presenta a los interesados los mecanismos de consentimiento, evitando ambigüedades, clarificando el medio o acción de la que se inferirá el consentimiento e intentando evitar la fatiga del usuario, ya que tal y como señala el Comité Europeo de Protección de Datos[27]: "En el ámbito digital, muchos servicios requieren datos personales para funcionar, de ahí que los interesados reciban cada día múltiples solicitudes de consentimiento que requieran una respuesta mediante un clic o deslizando el dedo por la pantalla. El

25 Directrices 5/2020 sobre el consentimiento…:
"i. la identidad del responsable del tratamiento,
ii. el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento,
iii. qué (tipo de) datos van a recogerse y utilizarse,
iv. la existencia del derecho a retirar el consentimiento,
v. información sobre el uso de los datos para decisiones automatizadas de conformidad con el artículo 22, apartado 2, letra c), cuando sea pertinente, e
vi. información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas, tal y como se describen en el artículo 46".
En idénticos términos, Considerando 42 del Reglamento (UE) 2016/679.

26 Aún tras la plena aplicación del Reglamento (UE) 2016/679 (25/05/2018) la Agencia Española de Protección de Datos, en su Guía sobre el uso de cookies, recogió el consentimiento diferido como un medio válido para expresar por el usuario su conformidad al uso de cookies. Dicha postura se corrigió, alineándose con el concepto de consentimiento inequívoco recogido por la normativa, en una segunda edición de la Guía sobre el uso de cookies publicada por el mismo organismo en 2020.

27 Ibidem.

resultado puede ser que el interesado se canse de hacer clic: si aparece demasiadas veces, el efecto real de advertencia de los mecanismos de consentimiento se va perdiendo. En consecuencia, las preguntas sobre consentimiento ya no se leen. Esto supone un riesgo especial para los interesados, ya que, habitualmente, el consentimiento se pide para acciones que son, en principio, ilegales sin dicho consentimiento. El RGPD impone a los responsables la obligación de desarrollar maneras de abordar este tema".

Asimismo, debe tenerse en cuenta que, cuando nos enfrentemos a un tratamiento que implique categorías especiales de datos, se precisará de un consentimiento "explícito"[28], cobrando especial relevancia ante la proliferación del uso de técnicas que implican el uso de datos biométricos para asegurar la identidad del interesado y evitar el repudio de la contratación (en esencia, reconocimiento facial y firma manuscrita electrónica).

Para finalizar, en lo que al consentimiento se refiere, deben tenerse en cuenta dos últimas notas predicables del consentimiento:

- De un lado, su carácter revocable, conforme a lo establecido en el artículo 7 apartado 3 RGPD[29], clarificando el Comité Europeo de Protección de Datos las garantías a tener en cuenta en el mundo online al señalar en las ya citadas directrices sobre el consentimiento "cuando el consentimiento se obtenga por medios electrónicos mediante un único clic del ratón, deslizando el dedo por una pantalla o pulsando una tecla, los interesados deben poder, en la práctica, retirar su consentimiento de manera igualmente sencilla. Cuando el consentimiento se obtenga mediante el uso de una interfaz de usuario específica de algún servicio, [por ejemplo, a través de un sitio web, una aplicación, una cuenta de inicio, una interfaz de un dispositivo de IdC (internet de las cosas) o por correo electrónico], no hay duda de que el interesado debe poder retirar el consentimiento a través de la misma interfaz electrónica, ya que cambiar a otra interfaz con el único fin de retirar el consentimiento requeriría un esfuerzo injustificado".

28 Ibidem: "El término explícito se refiere a la manera en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento. Una manera evidente de garantizar que el consentimiento es explícito sería confirmar de manera expresa dicho consentimiento en una declaración escrita. Cuando proceda, el responsable podría asegurarse de que el interesado firma la declaración escrita, con el fin de eliminar cualquier posible duda o falta de prueba en el futuro. No obstante, dicha declaración firmada no es el único modo de obtener el consentimiento explícito y no puede decirse que el RGPD prescriba declaraciones escritas y firmadas en todas las circunstancias que requieran un consentimiento explícito válido. Por ejemplo, en el contexto digital o en línea, un interesado puede emitir la declaración requerida rellenando un impreso electrónico, enviando un correo electrónico, cargando un documento escaneado con su firma o utilizando una firma electrónica".

29 Art. 7 apartado 3 RGPD: "El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo".

- De otro lado, que el principio de responsabilidad proactiva exige a los responsables del tratamiento la capacidad de acreditar sus niveles de cumplimiento, aspecto que alcanzaría a la acreditación de la obtención en sí misma del consentimiento, del alcance de dicho consentimiento y de la información proporcionada al interesado/ titular de los datos; detectándose, en demasiadas ocasiones, una absoluta incapacidad de los responsables para evidenciar cuándo y como se obtuvo el consentimiento.

IV.- EL DATO COMO ACTIVO

Cada vez en mayor medida, todo tipo de organizaciones con independencia de su tamaño y sector de actividad van otorgando un mayor peso a la información y a los datos personales como valor estratégico y activo esencial sobre el que, no sólo, se sustentaran sus procesos de negocio, sino que, a su vez, posibilitará la optimización de dichos procesos y mejorará su competitividad, contribuyendo, en definitiva, en la obtención de mejores resultados.

Recuperando la referencia a la sentencia del Tribunal Constitucional alemán en la que situamos el origen del derecho a la protección de datos en el ámbito europeo "un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia, y en esa medida ya no existe, bajo las condiciones de elaboración automática de datos, ningún datos sin interés"[30], dejando así patente la potencialidad y el valor de los datos; lo que nos sitúa ante un escenario de mercantilización de los datos, en el que las organizaciones son consumidoras de datos y, como tales, aceptan el dato como medio de pago.

Un conjunto de datos correctamente estructurado enriquecerá los procesos de toma de decisiones de las organizaciones, redundando en el logro de los objetivos y la obtención de mejores resultados, pues nos permitirá adecuar la oferta al consumidor, estudiar y subsanar las deficiencias del servicio y proceder a su optimización; incluso, a través de la utilización de tecnologías como Big Data seremos capaces de adelantarnos y predecir futuras necesidades y tendencias del mercado; así, por ejemplo, encontramos la serie "House of Cards" producida por la plataforma Netflix a partir de los resultados obtenidos de un algoritmo de análisis de los gustos y preferencias que habían venido mostrando sus propios usuarios; o, como la cadena de supermercados americanos Walmart descubría, a través de la minería de datos, un curioso patrón de ventas que consistía en que las ventas de tartas de fresa se multiplicaban por siete antes de un huracán.

30 El derecho a la protección de datos personales en la sociedad de la información. Herrán Ortiz A.I.: "El derecho a la protección de datos personales en la sociedad de la información" Cuadernos Deusto de Derechos Humanos, núm. 26, 2003, p. 14. Traducción de Daranas Peláez, M.: "Jurisprudencia constitucional extranjera. Tribunal Constitucional alemán. Ley del Censo". Boletín de Jurisprudencia Constitucional, núm. 33, 1984, p. 155.

Si bien es el mercado digital donde se produce la captación de esas informaciones, y, en general, donde se consume dicha información, finalmente, cualquier tipo de organización podrá convertirse en consumidora de datos, pues las técnicas de data science permitirá extraer información muy valiosa para todo tipo de organizaciones. Aunque, en ocasiones, se trabaja sobre datos estadísticos (e, irreversiblemente, disociados), las organizaciones deben prestar especial atención al origen legítimo de dichos datos y, en su caso, al cumplimiento de los requerimientos/ deberes de información que se establecen para con el interesado, cuando los datos no hayan sido proporcionados por el propio interesado.

Como consecuencia de ese creciente interés de las organizaciones en los datos personales, se vienen planteando numerosos contenidos y servicios a los que el usuario accede de forma gratuita o, mejor dicho, sin contraprestación económica, hablándose del dato personal como medio de pago y dándose la circunstancia de que el usuario, en gran parte de los casos, no es ni mínimamente consciente, no sólo de la repercusión de la difusión de los datos (sobre-exposición en redes sociales), sino que tampoco son conscientes "de que los facilitan ni para qué exactamente; la imposible equivalencia entre dinero y datos, pues dar los *últimos no priva al titular de darlos a otra persona ni es posible determinar el valor generado* con sus datos, a efectos de la obligación de restitución"[31].

La generalización de internet y, muy especialmente, del uso de los smartphones, conlleva a su vez la generalización de aplicaciones como Google, Gmail, Facebook, Instragram, Tik Tok, Wallapop, y un largo etcétera, que ofrecen servicios gratuitos a los usuarios, a los que deben añadirse múltiples dispositivos electrónicos y aplicaciones informáticas vinculadas a dichos dispositivos permanentemente receptivas a la captación de todo tipo de informaciones: localización, constantes vitales, actividad física, consumos, contactos, intereses, etcétera; pero, ¿Son realmente gratuitos estos servicios?, ¿Cómo obtienen sus grandes resultados estas organizaciones? La respuesta está en la venta de datos generales sobre los usuarios, sobre sus intereses, su actividad en la red. Pero, ¿Sabemos exactamente qué tipo de datos se venden? Gran parte de las políticas de privacidad que se examinaron por la AEPD, coinciden en que la cesión de datos hacia terceros versará sobre datos anónimos; no obstante, debe tenerse en cuenta que la aparición y el uso de técnicas como Big Data conlleva un gran riesgo de reidentificación de los interesados[32].

31 Sancho López, M.: "El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?", *InDret* 1, 2018.

32 González Guerrero, L. D.: "Control de nuestros datos personales en la era del Big Data: el caso del rastreo web de terceros", *Revista Estudios Socio-Jurídicos*, vol. 21, núm. 1, 2019, pp. 209-244. Universidad del Rosario – "(…) existen diversos estudios que demuestran la facilidad de correlacionar datos para particularizar una persona y conocer diversos aspectos de su vida privada, como opiniones y creencias políticas".

La mercantilización de los datos ha conllevado la aparición de novedosas profesiones, como son los data brokers o corredores de información, cuya actividad consiste en la recopilación de datos personales que, posteriormente, venderán, y, por consiguiente, nuevos mercados, los llamados "Data Marketplace"; tratándose de un negocio en pleno despegue y cuyo volumen de negocio se situó en 2019 en los 26 billones de dólares[33].

Así, ante esta creciente mercantilización de los datos personales, su valor indeterminado y la inconsciencia de los usuarios sobre captación, el legislador europeo ha incorporado en la normativa relativa a contratos de suministro de contenidos y servicios digitales mención expresa al dato como medio de pago[34], extremo que parece entrar en colisión con lo establecido en el artículo 7 apartado 4 RGPD respecto a las condiciones para el consentimiento cuando señala que, al analizar la libertad del consentimiento "se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato"[35]; planteándose por ello como reto añadido a los derivados del uso de tecnologías emergentes, la conjugación entre la nueva realidad del dato como medio de pago y su debida protección.

La Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019 tiene su transposición en el ordenamiento jurídico nacional, a través del Real Decreto – ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores; que entrará en vigor el 1 de enero de 2022, pretendiendo dar respuesta a una realidad cada

33 Daria R.: "El futuro de los mercados de datos", 31 de diciembre de 2019, https://rubygarage.org/blog/big-data-marketplaces

34 Ver art. 3 apartado 1 de la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales "La presente Directiva también se aplicará cuando el empresario suministre o se comprometa a suministrar contenidos o servicios digitales al consumidor y este facilite o se comprometa a facilitar datos personales al empresario, salvo cuando los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales con arreglo a la presente Directiva o para permitir que el empresario cumpla los requisitos legales a los que está sujeto, y el empresario no trate esos datos para ningún otro fin".

35 Pronunciamiento que se recoge en el art. 6 apartado 3 LOPDGDD: "No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual".

vez más generalizada, tal y como señala en su Exposición de Motivos[36], y extender la aplicación de la protección de la normativa de consumo a esta nueva realidad[37].

El uso que se prevé realizar de esos datos personales objeto de comercio, su potencialidad y las implicaciones que pueden derivarse para los propios titulares de los datos personales son, en gran medida, desconocidas; planteándose como un nuevo reto para el legislador, que deberá conjugar los ámbitos de protección, tanto de la normativa de protección de datos de carácter personal como de la normativa de consumo[38]; pues más allá de un inocente perfilado para ofrecernos el producto que más se ajusta a nuestros intereses, deberíamos plantearnos si ese conocimiento tan profundo que puede alcanzarse del sujeto a través de los numerosos datos que, de una u otra forma, lanzamos a la red permitirá:

- Determinar qué vamos a hacer o como vamos a actuar dadas ciertas circunstancias.

- Determinar si serán capaces de condicionar nuestras elecciones.

- Y si podrán afectar a diferentes ámbitos de nuestra vida personal y profesional, generándose problemas de discriminación a partir del análisis de nuestros datos personales, como podría ser la pérdida de oportunidades laborales o las negativas de contratación de servicios financieros o de aseguramiento, entre otros.

Esa diversidad de usos y las consecuencias que pueden presentarse para los titulares de los datos, especialmente, el hecho de que se esté sobrepasando la línea del perfilado hacia el condicionamiento, debería de centrar el debate sobre el ordenamiento jurídico actual y los necesarios límites que deben imponerse ante una situación, cuanto menos, preocupante; pero, es difícil obtener protección de

36 Exposición de Motivos del Real Decreto- Ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención de blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores: "Esta modalidad, cada vez más habitual en el mercado digital, debe tener en cuenta que la protección de datos personales es un derecho fundamental, por lo que los datos personales no pueden considerarse mercancía y su tratamiento debe cumplir las obligaciones aplicables e conformidad con el 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".

37 Ibidem: "Estos contratos han cobrado gran relevancia en los últimos años, sin que la normativa de consumo se haya adaptado a sus particularidades. En este contexto, es preciso tener en cuenta que los contenidos o servicios digitales se suministran también cuando el consumidor no paga un precio como tal, pero facilita datos personales al empresario. Estos contratos no cuentan en la actualidad con regulación específica, pues la consideración tradicional de contrato no contemplaba estos supuestos. Es por ello urgente y necesario cubrir este vacío, tanto por la necesidad de tener un marco jurídico estable y armonizado a nivel de la Unión Europea al respecto, como por la necesidad de ofrecer a los consumidores o usuarios una protección integral en sus distintas formas de contratación".

38 Helberger, N.: "Profiling and targeting consumers in the Internet of Things - A new challenge for consumer law", 6 de febrero de 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717

quien puede verse beneficiado por la situación, pues solo hace falta recordar la particularidad que supone que un ordenamiento jurídico en el que se estima que el consentimiento expreso de los interesados no será suficiente para levantar la prohibición general de tratamiento de ciertos datos de categorías especiales (entre ellos, aquellos relativos a la ideología)[39], diese a su vez cabida a que los partidos políticos pudiesen recopilar información de páginas web y redes sociales, elaborar bases de datos y contactar con los interesados afectados, sin su consentimiento previo. Dicha prerrogativa concedida a los partidos políticos llego al Tribunal Constitucional[40], que, dando prevalencia al derecho fundamental a la protección de datos de carácter personal, determinó que, si bien es lícito que los partidos políticos conozcan las tendencias de la población para decidir su estrategia y agenda política, en ningún caso podrá entenderse que esos "legítimos intereses" amparen tratamientos abusivos, desproporcionados y tendentes a orientar la voluntad del electorado[41].

Lo anterior, perfectamente, podría trasladarse al ámbito privado y deja patente que la tendencia actual sobrepasa el interés de las organizaciones de, simplemente, conocer ciertas informaciones sobre la población (ya sea en su conjunto o referida a un público concreto de un producto/ servicio); enfocándose los esfuerzos hacia predecir, determinar y controlar el comportamiento humano, pasando esta capacidad prácticamente desapercibida para gran parte de la población[42]; debiendo plantearnos una última pregunta, ¿Consumimos, escuchamos, vemos, leemos lo que queremos? Y más importante aún, ¿Podemos ver la realidad por nosotros mismos o solo vemos lo que nos muestran? ¿Tenemos un pensamiento propio o condicionado?

Para finalizar y, en cierta medida sino afianzar si al menos dotar de contenido las preguntas anteriormente planteadas y traerlas desde la ciencia ficción a la

39 Art. 9 apartado 1 LOPDGDD: "A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. (…)".

40 STC 76/2019, de 22 de mayo 2019, (RTC 2019,76). Recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo respecto del apartado primero del art. 58 bis de la LOPDGDD, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Protección de datos personales, principio de seguridad jurídica, vertiente negativa de la libertad ideológica y derecho a la participación política: nulidad del precepto legal que posibilita la recopilación por los partidos políticos de datos personales relativos a las opiniones políticas de los ciudadanos.

41 Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

42 Schneier, B.: Datos y Goliat. Las batallas ocultas para recopilar tus datos y controlar tu mundo, 2015. Nueva York: WW Norton & Company: "la manipulación psicológica, basada en la información personal y en el control de los sistemas, solo mejorará. Peor aún, será tan buena, que no nos daremos cuenta de su presencia".

realidad, nada mejor que un claro ejemplo real, tanto de la potencialidad de los datos personales estructurados como del interés que despiertan en todo tipo de organizaciones y de la falta de conocimiento y de control sobre su uso por parte de los interesados: el escándalo de Cambridge Analytica. En 2013, la entidad Cambridge Analytica promovió, a través de la aplicación Facebook, el desarrollo de un test de personalidad a través del que se recopilaron datos de más de 250.000 personas, en general, ciudadanos americanos y, a su vez, de los contactos de éstos (sin el consentimiento de éstos últimos), concretamente, se captaron datos sobre actualizaciones de estados, "likes", e, incluso, mensajes privados, con un alcance final estimado del 15% de la población de Estados Unidos. Los datos obtenidos a través del citado test, posteriormente, fueron vendidos a una tercera entidad que, usando técnicas de perfilado, logró perfiles psicológicos que resultaron de vital importancia para una última y preocupante acción, el condicionamiento del voto de los afectados a través del llamado "dominio informativo", durante la campaña a la presidencia norteamericana que enfrentó a Donald Trump como Hillary Clinton. Ese dominio informativo, conforme a las explicaciones dadas desde la propia entidad, es invisible e imperceptible, y consiste en controlar todas las fuentes de información que rodean al sujeto, y de esta forma influir en la forma en la que se comportarán y reaccionaran, esto es, en que votarán.

V.- CONCLUSIÓN

A mi juicio, el uso masivo continuo de internet y de aplicaciones ofreciendo servicios gratuitos a los usuarios conlleva una obtención de todo tipo de información indirecta para las organizaciones sin que los consumidores sean conscientes de la importancia que tienen sus datos como materia prima, convirtiéndose actualmente, su tratamiento en mercancía para las empresas, por ello, es urgente que el suministro de contenidos digitales cuente a su vez con regulación específica que garantice los derechos de los consumidores o usuarios en este ámbito pero interrelacionada a la vez con la regulación específica de la protección de datos, de manera tal que no se consiga influir en el comportamiento del ser humano cuando consume.