NUEVA MONEDA DE CAMBIO:
NUESTROS DATOS PERSONALES COMO PAGO DE CONTENIDOS DIGITALES[1]

Mª Nieves Pacheco Jiménez[2]
Prof. Contratada Doctora
(Titular Acreditada)
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Mikael Leal Coronado
Máster en Acceso a la Abogacía
Becario de Colaboración Dpto. Derecho Civil
Universidad de Castilla-La Mancha

Fecha de publicación: 13 de junio de 2017

1. UN NUEVO MODELO DE NEGOCIO

Los estudios elaborados hasta ahora por CESCO en el ámbito de la denominada revolución digital en el concreto ecosistema de los medios de pago tenían como premisa un intercambio basado en dinero electrónico o en criptodivisas. Sin embargo, asistimos al desarrollo de un nuevo modelo de negocio en el que las empresas ofrecen servicios y contenidos digitales a sus usuarios a cambio de datos personales[3]. Estos datos son manejados por grandes empresas tecnológicas con el objetivo de que gigantes como Google, Facebook[4], Amazon o Microsoft los exploten oportunamente. Ello dará lugar al "efecto de red de datos", esto es, usar los datos

[1] Trabajo realizado en el marco de la Ayuda del Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia (Subprograma Estatal de Generación de Conocimiento) del Ministerio de Economía y Competitividad, otorgada al Grupo de investigación y Centro de investigación CESCO, Mantenimiento y consolidación de una estructura de investigación dedicada al Derecho de consumo, dirigido por el Prof. Ángel Carrasco Perera, de la UCLM, ref. DER2014-56016-P.

[2] ORCID 0000-0002-9062-2342

[3] IDC, una firma de estudios de mercado, señala que el "universo digital", entendido como los datos creados y copiados cada año, llegará a los 180 zettabytes (180 seguido de 21 ceros) en 2025.
Vid. https://remasa.com/es/blog/c%C3%B3mo-los-datos-se-convertir%C3%A1n-en-el-petr%C3%B3leo-del-futuro

[4] Concretamente, Facebook y Google inicialmente usaron los datos que recogían de los usuarios para orientar mejor su publicidad, pero en los últimos años han ido más allá en su uso potencial ya que esos datos pueden convertirse en servicios de inteligencia artificial o cognitivos (v. gr., traducción, reconocimiento visual, evaluación de la personalidad), lo que puede llevar aparejada una valoración económica.
Vid. https://remasa.com/es/blog/c%C3%B3mo-los-datos-se-convertir%C3%A1n-en-el-petr%C3%B3leo-del-futuro

para atraer más usuarios, que entonces generarán más datos y mejorarán los servicios, captando a más usuarios[5].

En verdad esta práctica resulta incoherente con el temor del usuario de Internet de no proteger adecuadamente su privacidad ya que el "pago" por disfrutar de las aplicaciones ofrecidas no es otro que poner a disposición de las empresas sus datos personales.

Atendiendo a esta situación, y en aras de proporcionar una adecuada regulación en este controvertido ámbito, en diciembre de 2015 la Comisión Europea presentó una propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales[6].

2. LOS CONTENIDOS DIGITALES

En primer lugar, es necesario saber qué son los denominados "contenidos digitales". El artículo 2.1 de la propuesta de Directiva entiende por tales: "a) datos producidos y suministrados en formato digital, por ejemplo vídeo, audio, aplicaciones, juegos digitales y otro tipo de software; b) servicio que permite la creación, el tratamiento o el almacenamiento de los datos en formato digital, cuando dichos datos sean facilitados por el consumidor; c) servicio que permite compartir y cualquier otro tipo de interacción con datos en formato digital facilitados por otros usuarios del servicio". Es interesante reseñar que la norma se refiere no solo a los contenidos digitales suministrados por proveedores, sino también a aquellos otros que el consumidor facilite o almacene durante el período de duración del contrato (v. gr., música, archivos de vídeo, fotografías, juegos)[7].

Asimismo, y de conformidad con el Considerando 11 de la propuesta de Directiva, "si bien existen numerosas formas de suministrar contenidos digitales, como la transmisión en un soporte duradero, la descarga por los consumidores en sus dispositivos, la transmisión a través de la web, el permiso para acceder a capacidades de almacenamiento de contenidos digitales o el acceso al uso de redes sociales, la presente Directiva debe aplicarse a todos los contenidos digitales con independencia del soporte utilizado para su transmisión".

Sin embargo, uno de los factores que limita a los consumidores para adquirir contenidos digitales es la inseguridad sobre sus derechos contractuales básicos, lo que pretende ser minimizado con una adecuada regulación a través de la Directiva correspondiente. Así, y atendiendo a su Considerando 6, "unas normas plenamente armonizadas específicas para los contenidos digitales para toda la UE eliminarán la complejidad generada por las diferentes normativas nacionales aplicadas en la actualidad a los contratos de suministro de contenidos

[5] *Vid*. https://remasa.com/es/blog/c%C3%B3mo-los-datos-se-convertir%C3%A1n-en-el-petr%C3%B3leo-del-futuro

[6] COM (2015) 634 final; 2015/0287 (COD)
Para un estudio más completo sobre la misma, *vid*. MILÀ RAFEL, R.: "Intercambios digitales en Europa: Las propuestas de Directiva sobre compraventa en línea y suministro de contenidos digitales, en *Revista CESCO de Derecho de Consumo*, Nº 17, 2016.

[7] MILÀ RAFEL, R., *op. cit*, p. 29.

digitales". Añade su Considerando 7 que los consumidores "contarán con derechos claros cuando reciban o accedan a contenidos digitales desde cualquier lugar de la UE", lo que "fomentará su confianza a la hora de comprar contenidos digitales" y "contribuirá a reducir los perjuicios que sufren actualmente los consumidores, ya que existirá un conjunto de derechos claros que les permitirán abordar los problemas a los que se enfrentan con los contenidos digitales".

3. INTERCAMBIO DE CONTENIDOS DIGITALES POR DATOS PERSONALES

Como señalábamos al principio de este estudio, la contraprestación habitual en el ecosistema digital se basa en un precio (v. gr., dinero electrónico, criptodivisas). Sin embargo, resulta destacable en la propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales que su regulación se aplique también a aquellos contratos en los que la contraprestación no es dineraria, sino consistente en datos personales u otro tipo de datos que el proveedor solicita y el consumidor facilita activamente[8].

Lo cierto es que los mercados de datos personales no son algo nuevo; los "Data brokers"[9] llevan tiempo comercializando ciertos tipos de datos. La cuestión no se centra en almacenar dichos datos, sino en procesarlos y entenderlos, construyendo modelos de comportamiento que posteriormente venden al mejor postor[10]. Sin embargo, las grandes empresas tecnológicas han descubierto la potencialidad del procesamiento de estos datos ya que pueden convertirse en servicios de inteligencia artificial o cognitivos (v. gr., traducción, reconocimiento visual, evaluación de la personalidad), susceptibles de valoración económica[11].

Esta modalidad va cobrando relevancia paulatinamente, lo que genera en la práctica una diferenciación en función de la naturaleza de la contraprestación y, por ende, una discriminación entre los diferentes modelos de negocio, en tanto en cuanto las empresas tendrían un incentivo injustificado para orientarse hacia la oferta de contenidos digitales a cambio de datos. Esta preocupación se refleja en el Considerando 13 de la propuesta de Directiva, por lo que aboga por garantizar unas condiciones equitativas.

Pero el problema va más allá… Los consumidores y los gigantes tecnológicos no acaban de saber cómo manejar esos datos y cuál es su verdadero valor (esto no es más que la punta del iceberg), sin desdeñar la mecánica habitual derivada del propio desconocimiento, que lleva a

---

[8] Art. 3.1: "*La presente Directiva se aplicará a cualquier contrato en virtud del cual el proveedor suministra contenidos digitales al consumidor o se compromete a hacerlo y, a cambio, se paga un precio o el consumidor facilita activamente otra contraprestación no dineraria en forma de datos personales u otro tipo de datos*".

[9] En Europa hay alrededor de 50 grandes empresas "Data brokers".
Vid. http://tecnologia.elpais.com/tecnologia/2017/05/03/actualidad/1493835469_309268.html

[10] *Vid*. http://www.abc.es/tecnologia/informatica-software/20140713/abci-comercio-datos-internet-data-broker-cookies-201407111531.html

[11] Empresas como Citizenme o Datacoup permiten a sus usuarios obtener una pequeña suma si la comparten con marcas. *Vid*. https://remasa.com/es/blog/c%C3%B3mo-los-datos-se-convertir%C3%A1n-en-el-petr%C3%B3leo-del-futuro

los usuarios a aceptar por inercia los términos y condiciones de las aplicaciones con contenidos digitales.

Para salvaguardar los intereses del consumidor, señala la propuesta de Directiva en su Considerando 14 que la regulación se aplicará "sólo a los contratos en los que el proveedor solicita y el consumidor facilita datos de forma activa, como el nombre y la dirección de correo electrónico o fotos, directamente al proveedor". Por tanto, "la presente Directiva no debe aplicarse a las situaciones en las que 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[12], por ejemplo cuando el registro del consumidor es necesario por motivos de seguridad e identificación en virtud de la legislación aplicable", ni "tampoco debe aplicarse a situaciones en las que el proveedor recaba información, incluidos datos personales, tales como la dirección IP u otra información generada automáticamente como información recogida y transmitida por una *cookie*, sin que el consumidor la facilite activamente, aunque el consumidor acepte la *cookie*"; por último, "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".

Esta contraprestación en forma de datos personales no está exenta de polémica, sobre todo cuando el escrito regulatorio original posibilitaba que los usuarios pudieran comerciar con sus datos personales a cambio de recibir contenidos y servicios digitales gratuitamente[13]. Esto provocó que el propio Supervisor Europeo de Protección de Datos (SEPD) presentara un dictamen en contra señalando que los datos personales "no pueden concebirse como un mero activo económico" y, por tanto, "no deberían ser tratados como contraprestación contractual del consumidor en lugar de dinero". Lógicamente esta crítica enlaza con la protección de derechos fundamentales, que, en su vertiente de datos personales, no puede reducirse a una "mera mercancía".

Sin embargo, y atendiendo a expertos en la materia[14], la postura del SEPD no sería correcta en la medida en que parte de una perspectiva errónea. Y ello porque la normativa de protección de datos pivota sobre el consentimiento informado, inequívoco y previo del titular de los datos, siempre bajo el cumplimiento de determinados requisitos de seguridad. Pero, además, se considera una vía más: la vertiente económica del derecho fundamental. En ese sentido, si otros derechos fundamentales, como la intimidad, el honor y la propia imagen, son explotables económicamente, ¿qué sentido tendría limitarse cuando se trata de datos personales?

4. REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

[12] Art. 3.4
[13] Noticia Expansión Jurídico: "¿Puedo utilizar mis datos como moneda de cambio", 26 mayo 2017.
[14] *Ibídem*.

4.1. Contextualización

En este punto procede centrarse en la protección dispensada por el ordenamiento jurídico europeo en sede de tratamiento de datos de carácter personal. Y ello en relación con el contenido de la propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales. En su Considerando 22 establece que "la protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE del Parlamento Europeo y del Consejo y por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo que son plenamente aplicables en el contexto de los contratos de suministro de contenidos digitales"; "dichas directivas ya establecen un marco jurídico en el ámbito de los datos de carácter personal en la Unión", por lo que "la aplicación e implementación de la presente Directiva debe realizarse cumpliendo plenamente dicho marco jurídico". Igualmente, su art. 3.8 señala que "*la presente Directiva debe entenderse sin perjuicio de la protección de las personas con respecto al tratamiento de datos de carácter personal*".

Sin embargo, a fecha de hoy está en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[15], 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.

Partiendo de esta premisa, el mencionado Reglamento, aprobado tras años de negociaciones, y reflejo de la enorme importancia que otorga la Unión Europea a los datos personales, que implica una concienciación a nivel global en materia de privacidad de personas y empresas[16], "pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas" (Considerando 2). Y ello porque "la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales", pues la magnitud de la recogida y del intercambio de datos personales ha crecido de manera significativa, permitiendo la tecnología que tanto las empresas privadas como las autoridades públicas utilicen los datos personales en una escala sin precedentes cuando lleven a cabo sus actividades, atendiendo al Considerando 6.

Tanto es así que la integración económica y social que resulta del funcionamiento del mercado interior ha contribuido a un incremento sustancial de los flujos transfronterizos de los datos personales, cuyo intercambio ha aumentado en toda la Unión entre los operadores públicos y privados, incluyendo a las personas físicas, las asociaciones y las empresas, como se desprende del Considerando 5.

[15] DOUE, núm. 119, de 4 de mayo de 2016.
[16] *Vid.* https://www.apdtic.com/novedades-del-nuevo-reglamento-europeo-de-proteccion-de-datos/

Es patente que cada vez más las personas difunden una gran cantidad de información personal a escala global, ya que "la tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales" (Considerando 6).

Así las cosas, para generar la confianza necesaria que permita un elevado desarrollo de la economía digital en el mercado interior se requiere un marco todavía más sólido y coherente, imprescindible para la protección de nuestros datos en la Unión Europea, que cuente una estricta ejecución, siendo necesario que las personas físicas tengan en todo momento el control de sus propios datos personales, reforzando la seguridad jurídica y la práctica en conjunto para las personas físicas, operadores económicos y autoridades públicas, como establece el Reglamento en su Considerando 7.

Además, constituye una exigencia para la protección adecuada de los datos personales en la Unión "que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes" (Considerando 11), teniendo en cuenta que "el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales" (Considerando 13). Y en relación a este tratamiento, "para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento [...]"; reconociendo también "un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales -"datos sensibles"-" (Considerando 10).

Sin perjuicio de todo lo anterior, y dado que el objetivo de este Reglamento es garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, al no poder alcanzarse de manera suficiente por parte de los Estados miembros, y ya que, debido a las dimensiones de la acciones, este objetivo puede conseguirse mejor a escala de la Unión, ésta podrá adoptar medidas, de conformidad con el principio de subsidiariedad establecido en el artículo 5 del Tratado de Funcionamiento de la Unión Europea, pues así se ha hecho constar en el Considerando 170 del Reglamento.

4.2. Principales novedades y aspectos esenciales

Con el fin de lograr el objetivo antes mencionado, esto es, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, el presente Reglamento plantea un triple objeto en su artículo 1, a saber:

- *"Establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos".*

- *"Protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales".*

- *"La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".*

A raíz de ello, resulta relevante él ámbito de aplicación, tanto material como territorial, del Reglamento. Respecto al primero, el art. 2.1 señala que *"se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"*, con las exclusiones previstas en su apartado segundo. Y en relación al ámbito de aplicación territorial, se introduce como novedad su aplicación *"al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividad de tratamiento estén relacionadas con: la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o el control de su comportamiento, en la medida en que este tenga lugar en la Unión"*, como así se estipula en su art. 3.2. De manera que todas aquellas empresas que se encuentren situadas fuera de la Unión Europea, pero que proporcionen sus productos o servicios por medio de Internet a los ciudadanos europeos, tendrán que cumplir el Reglamento General de Protección de Datos[17].

Centrándonos en el tratamiento y protección propios de los datos personales, estos deberán ser manejados en base a una serie de principios, enunciados en su artículo 5, y que serían los siguientes:

- Tratamiento basado en la licitud, lealtad y transparencia en relación con el interesado.

- Limitación de su finalidad, por lo que serán recogidos con fines determinados, explícitos y legítimos, sin poder tratarse posteriormente de manera incompatible con los mencionados fines.

- Minimización de datos, siendo éstos adecuados, pertinentes y limitados a la necesidad de los fines.

[17] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD): "Protección de Datos: Guía para el Ciudadano".

- Necesidad de exactitud y, cuando sea necesario, actualización.

- Limitación en el plazo de conservación, permitiendo la identificación de los interesados, pero sin exceder del tiempo necesario para los fines del tratamiento de dichos datos.

- Importancia de la integridad y confidencialidad, de manera que en su tratamiento se garantice una seguridad apropiada de los datos personales, incluyendo la protección frente a un procesamiento que no haya sido autorizado o ilícito y frente a la pérdida, destrucción o daño accidental, siendo necesaria la aplicación de una serie de medidas técnicas u organizativas adecuadas.

Además de estos principios, será preciso cumplir alguna de las condiciones establecidas en el art. 6.1 del Reglamento para que el tratamiento de los datos sea lícito, a saber: a) que el interesado haya dado su consentimiento[18] para el tratamiento de sus datos para uno o varios fines determinados; b) que el tratamiento sea necesario para la ejecución de un contrato en que sea parte el interesado o para la aplicación, a petición suya, de medidas precontractuales; c) que sea imprescindible para el cumplimiento de una obligación legal que resulte aplicable al responsable del tratamiento; d) que sea pertinente con el fin de protección de los intereses vitales del interesado u otra persona física; e) que sea necesario para el cumplimiento de una labor realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento; f) que sea obligatorio para la satisfacción de intereses legítimos que sean perseguidos por el responsable del tratamiento o por un tercero, y no prevalezcan los intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales, especialmente si el interesado es un niño.

En relación a la importancia de la información, conviene recordar que, de conformidad con el art. 12.1 del Reglamento, el responsable del tratamiento tendrá que tomar las medidas adecuadas para facilitar al interesado la información a que hacen referencia sus artículos 13 y 14, además de cualquier comunicación, con arreglo a los artículos 15 a 22 –en los cuales se regulan pormenorizadamente los derechos de acceso, rectificación, supresión ("derecho al olvido"), a la limitación del tratamiento, a la portabilidad de los datos, oposición y a no ser objeto de decisiones individualizadas- y 34, en lo relativo al proceso, de una manera concisa, transparente, inteligible y de fácil acceso, especialmente en caso de que sea dirigida a un niño, pudiendo ser proporcionada la referida información por escrito o por otros medios, e incluso por medios electrónicos.

[18] Respecto al consentimiento del interesado éste se hará mediante una declaración o acción afirmativa, pues se entiende por tal consentimiento: "*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",* tal y como se establece en el art. 4.11 del Reglamento, y asimismo habrán de cumplirse las condiciones establecidas en sus artículos 7 y 8, respecto al mencionado consentimiento.

Del articulado del Reglamento resulta sustancial el papel desarrollado por el Delegado de Protección de Datos o DPO[19], que será necesario designar cuando el tratamiento lo lleve a cabo una autoridad u organismo público -salvo que los tribunales actúen en el ejercicio de su función judicial-, cuando las actividades del responsable o del encargado traten de operaciones de tratamiento que necesiten de una observación habitual y sistemática de los interesados a gran escala, o cuando las actividades del responsable o encargado versen sobre el tratamiento a gran escala de modalidades especiales de datos personales y de los relativos a condenas e infracciones penales (tal y como se establece en el art. 37.1 del Reglamento), y cuyas específicas funciones se establecen en su art. 39.

Otro de los puntos novedosos de este Reglamento es el referido a la evaluación de impacto relativa a la protección de datos y consulta previa, siendo ineludible cuando exista posibilidad de que un tipo de tratamiento, en concreto si se usan nuevas tecnologías, pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas; de manera que el responsable del tratamiento tendrá que realizar, antes del mismo, una evaluación del impacto que esas operaciones tengan en la protección de datos personales, de conformidad con lo establecido en el art. 35.1 del Reglamento.

Por lo que se refiere al régimen sancionador, éste ha sido reforzado, pudiéndose sancionar con multas administrativas que pueden llegar a alcanzar los 10.000.000 o 20.000.000 de euros como máximo, o en caso de que se trate de una empresa, de una cuantía equivalente al 2% o al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, en los casos previstos en los apartados 4 y 5 del art. 83 del Reglamento. A tenor de ello es evidente que este Reglamento va a obligar a todas las empresas y entidades a llevar a cabo la revisión de todas sus actuaciones y medidas de seguridad relativas a la protección de datos, de manera que se ajusten a las nuevas previsiones[20].

Para dar cumplimiento a estas y otras novedades recogidas a lo largo del articulado del nuevo Reglamento General de Protección de Datos, y según lo dispuesto en su art. 99.2, éste será aplicable a partir del 25 de mayo de 2018, siendo obligatorio en todos sus elementos y de aplicación directa en cada Estado Miembro, de manera que queda menos de 1 año para que los Estados culminen la preparación e interpretación de todas las obligaciones y derechos instituidos en el mencionado texto.

5. CONSIDERACIONES FINALES

Es evidente que los datos personales se están convirtiendo en una nueva forma de comerciar, sustitutiva de un precio en dinero, especialmente en aplicaciones y servicios de suministro de contenidos digitales. El verdadero pago de estos son los datos personales proporcionados por los usuarios a cambio de disfrutar de los citados servicios y contenidos digitales. En realidad,

[19] DPO, por sus siglas en inglés: *Data Protection Officer*.
[20] *Vid.* http://ecija.com/wp-content/uploads/2017/06/Sanciones-RGPD.pdf

el consumidor o usuario desconoce el auténtico potencial que pueden llegar a tener esos datos; cosa que no sucede con las empresas y portales electrónicos, conscientes de la utilidad de esta información, que les permitirá obtener, a su vez, más usuarios y beneficios.

Sin duda nos encontramos en un mero punto de partida, que seguirá desarrollándose hasta alcanzar altos niveles de información personal en la Red, y que será necesario controlar para una eficaz protección de los consumidores y usuarios. De ahí que sea especialmente importante que, antes de proporcionar nuestros datos y autorizar que sean utilizados, pensemos detenidamente y prestemos la debida atención a la política de privacidad y a los términos y condiciones (lo que rara vez se hace), al igual que comprendamos los derechos que podemos accionar en caso de un uso indebido de los datos personales por parte de las empresas y entidades.

Esperemos que el nuevo Reglamento General de Protección de Datos, a unos meses de ser directamente aplicable en nuestro país, refuerce e incremente el tratamiento, la protección y la seguridad de nuestros datos personales, además de promover la concienciación general sobre la importancia y las consecuencias que puede llegar tener la información personal en esta era digital, donde la mayoría de consumidores y usuarios están interconectados a través de los más variados dispositivos electrónicos.

En definitiva, es el consumidor/usuario quien decide qué datos personales está dispuesto a proporcionar como moneda de cambio para obtener cierto tipo de servicios y contenidos digitales. Ahora resta que entienda el uso que, a la postre, se puede hacer de ellos al aceptar (sin adoptar unas mínimas precauciones) los términos y condiciones prefijados por empresas y portales electrónicos.