diariolaley

Wolters Kluwer

Internet de las Cosas y tutela jurídica de recursos inmateriales

Sergio MIRALLES MIRAVET

Abogado en Intangibles Legal, SLP

Diario La Ley, Nº 7, Sección Ciberderecho, 29 de Mayo de 2017, Editorial **Wolters Kluwer**

Comentarios

I. INTRODUCCIÓN

Los derechos de propiedad industrial e intelectual (los «derechos IP») son probablemente una de las ramas de nuestro ordenamiento jurídico más sensible a los cambios tecnológicos. De hecho, innovaciones tecnológicas fueron la génesis de muchos de estos derechos, y su razón de ser en última instancia.

En la actualidad, probablemente estemos en un periodo que propicie transformaciones relevantes en los derechos IP.

De un lado, la consolidación del fenómeno digital y de la *World Wide Web*, que en menos de 20 años desde su irrupción ha pasado a ser un elemento consustancial a nuestras vidas, están llamadas a transformar la configuración de varios derechos IP.

De otro lado, las innovaciones de la ingeniería electrónica han propiciado un crecimiento geométrico de la capacidad de procesamiento de los sistemas de tratamiento de información, y han permitido la miniaturización de microprocesadores que son empleados como sensores para la captación de datos. Ello, acompañado a una reducción sustancial de los costes de dicho *hardware*, ha favorecido la implantación del conocido como «Internet de las cosas» (el «*IoT*»), una suerte de compañero del primigenio «Internet de las personas». **El IoT ha sido llamado por voces cualificadas a ser uno de los agentes de la llamada cuarta revolución industrial** (1) .

Es bien sabido que el IoT genera ingentes cantidades de datos que son posteriormente objeto de análisis mediantes técnicas novedosas. Esta es una de las principales fuentes informativas que nutren a los conocidos como datos masivos o *Big Data*.

La mayoría de los modelos de negocio en entornos de IoT y *Big Data* precisan del acceso constante a flujos de datos de orígenes diversos cuyo análisis permite la obtención de información con valor añadido. El tratamiento y análisis de datos en procesos de IoT y *Big Data* puede cualificarse por sus notas de gran volumen, velocidad disparidad del origen de los datos y fluidez del proceso.

Volumen, disparidad de origen y fluidez del proceso de entrada y salida (*input data – output information*) implican, a mi modo de ver, un punto de inflexión en el esquema clásico de protección de los derechos IP. Tradicionalmente los derechos IP se han centrado en dispositivos, formulaciones, composiciones, sistemas o procedimientos (supuestamente) bien definidos, expresados (*fixation*) y acotados, como contraprestación al monopolio temporal concedido. Dichas condiciones conceden seguridad jurídica a los operadores económicos que pueden de esta forma idear o desarrollar sus iniciativas evitando la infracción de derechos de exclusiva de terceros. Pues bien, el dinamismo del IoT y *Big Data* puede trastocar dichas notas.

En supuestos de IoT / *Big Data* podemos diferenciar diversos ámbitos (cuya ejecución puede solaparse temporalmente) en los que mediarían actividades intelectuales (humanas): (i) planteamiento general, es decir, determinación de los propósitos del tratamiento de datos y/o información, (ii) determinación de qué datos y/o información serán recogidos y cómo se recogerán, (iii) desarrollo del algoritmo o algoritmos que procesarán la información para realizar su análisis, (iv) interpretación de los resultados del análisis, (v) comprobación subsiguiente mediante experiencia empírica sobre los beneficios del proceso, y (vi) frecuentemente, reajuste o reconfiguración de alguno de los anteriores pasos para corregirlos o mejorarlos. A mi entender, las fases de mayor dificultad, y por tanto las que entrañarán mayor creatividad, son las tres primeras y especialmente el planteamiento inicial.

II. ELEMENTOS DEL IoT Y *BIG DATA* RELEVANTES DESDE EL PLANO LEGAL

La tutela jurídica de recursos inmateriales asociados a IoT y/o *Big Data* debe tener en cuenta, entre otros muchos y sin orden de importancia, los siguientes aspectos:

a) Conectividad: necesidad de que las autoridades de regulación adopten estrategias lo más coordinadas posible en cuestiones como gestión de espectro radioeléctrico, estándares y *roaming* para facilitar la implantación internacional de servicios de IoT y/o *Big Data.*

b) Interoperabilidad y estandarización: los múltiples dispositivos del IoT deben poder comunicarse y, por ello, es preciso emplear estándares y protocolos de comunicación. Las redes móviles de 5ª generación, actualmente en desarrollo, deben todavía dotarse de estándares y especificaciones. Los organismos de estandarización deben tener presentes cuestiones relacionadas con derechos de IP, entre las que destacan las obligaciones de divulgación de patentes esenciales (SEPs) y oferta de licencias a los usuarios del estándar en términos FRAND (*i.e.,* justos, razonables y no discriminatorios).

c) Portabilidad: entendida como capacidad del cliente de migrar sus datos entre prestadores de servicios. El Reglamento (2016/679) General de Protección de Datos (el «GDPR») crea un nuevo derecho a la portabilidad de datos personales que se configura como un derecho al acceso a los datos en «un formato estructurado, de uso común y lectura mecánica». Este nuevo derecho, junto con otros de nuevo corte como el «derecho al olvido», tiene una clara vocación de aplicación en entornos de Internet.

d) Multipolaridad: muchas bases y flujos de datos se nutren de fuentes con origen en individuos, entidades o dispositivos diversos. Ese origen múltiple dificulta la tutela jurídica de recursos inmateriales conformados por ese crisol de datos e información.

e) Plataformas de intermediación: muchos servicios innovadores en ámbito del IoT y/o *Big Data* precisan de la colaboración de grandes plataformas que intermedian entre el prestador del servicio y los usuarios finales (a su vez, clientes de la plataforma). Esta (relativamente nueva) figura suscita cuestiones de orden contractual (*e.g.* condiciones de acceso a datos y a clientes, responsabilidad, etc.) y legal (*e.g.* posible posición de dominio en el mercado específico).

f) *Application Programming Interfaces* (las «APIs»): Las APIs son un conjunto de protocolos y rutinas que permiten una fácil interoperabilidad entre aplicaciones o páginas *web*, entre otros. Es decir, sirven de puente para que diferentes servicios puedan comunicarse entre sí con facilidad. Entre las APIs más conocidas se encuentran la API de Google Maps que permite integrar los mapas en las páginas web de terceros o las APIs de eBay y Amazon. Otras APIs simplemente proporcionan una forma sencilla de acceso por parte de terceros a una determinada base de datos, como por ejemplo la disponibilidad y precio de vuelos de las aerolíneas. Las APIs juegan un papel clave en las tecnologías de minería de texto y datos (*text and data mining*), actualmente en pleno debate legislativo en el Parlamento Europeo en el contexto de la actualización del *acquis* de derechos de autor.

g) *Open* Software: la mayoría de prestadores de servicios en entornos de IoT y *Big Data* desarrollan software específico de una forma mucho más ágil y dinámica que hace una década. Y lo hacen empleando, total o parcialmente, *open software*, entendido éste como software desarrollado por terceros que se pone a disposición de todos los usuarios interesados que son libres de utilizarlo para integrarlo en sus desarrollos y distribuirlo a terceros bajo los términos de licencia de ese software. Una de las mayores ventajas de este tipo de software es la disponibilidad del código fuente. Con todo, su uso obviamente no está exento de riesgos como, según el caso, la necesidad de puesta a libre disposición de desarrollos internos en los que ha mediado código abierto o la necesidad de aplicar controles internos más estrictos que cuando se licencia software «propietario».

h) Impresión 3D y nuevos formatos de ficheros: se consolida la evolución del empleo de ficheros con diseños en 2D a ficheros con definición de modelos 3D (*Model-based definition* o MBD). Ello probablemente genere nuevas cuestiones en materia de infracción indirecta de algunos derechos IP, como por ejemplo sobre diseños industriales (2) .

i) Algoritmos: los ordenamientos jurídicos han evitado conceder derechos IP a métodos matemáticos, algoritmos y a los planes, reglas y métodos para el ejercicio de actividades intelectuales o económico-comerciales (*cfr.* art. 4 a) y c) Ley 24/2015 de Patentes). Ello se debe a su consideración como recursos que, por cuestiones de orden público, deben permanecer fuera del ámbito de los derechos de exclusiva. No

obstante, la aplicabilidad industrial de algoritmos se ha incrementado exponencialmente en las últimas dos décadas, siendo una de las piezas angulares del IoT. La proliferación del desarrollo de algoritmos (cada vez más complejos) ha venido acompañada de un creciente interés en su protección legal de manera indirecta (patentes, derechos de autor sobre software…) o directas (secretos industriales).

j) Los datos e información como materia prima del IoT: por motivos parecidos respecto a los algoritmos, la información y los datos desestructurados no han sido tradicionalmente objeto de derechos IP, al menos considerados en sí mismos (3) (*cfr.* considerandos 45 y 46 Directiva 96/9/CE, art. 10.2 *in fine* ADPIC o art. 2.8 Convenio de Berna de 1886). Se produce en este ámbito un choque de intereses: de un lado el público respecto a la libre circulación de la información (cfr. Directiva 2003/98/EC sobre reutilización de la información en el sector público), y de otro el privado respecto a la obtención de algún tipo de exclusiva respecto a los datos generados por iniciativa privada (4) . No parece fácil (ni a mi entender, conveniente) la creación de un nuevo derecho de IP *sui generis* que otorgue algún tipo de derecho de exclusiva sobre datos e información. Además de razones de interés público en la libre circulación de datos, la propia configuración compleja de muchas bases de datos con pluralidad de orígenes hacen difícil la asignación de reglas claras de asignación de dominio; pensemos, por ejemplo, en cadenas de datos (*data strings*) como el *passanger name record* (PNR) de un viajero, formadas por diversos eslabones y generadas por partes distintas en momentos distintos. En consecuencia, la protección mediante secreto industrial y la regulación contractual parecen los principales, sino únicos, métodos disponibles en la actualidad para proteger y regular los datos e información en contextos de IoT / *Big Data*.

k) Tecnología al servicio del *enforcement:* la rapidez y dinamismo que acompañan a los desarrollos tecnológicos relacionados con IoT / *Big Data* han propiciado que los operadores del mercado busquen alternativas «técnicas» que contribuyan o complementen sus necesidades de protección legal. Las medidas tecnológicas de protección anti-copia o los sistemas informativos de gestión de derechos (TPM y DRM en sus acrónimos ingleses) aparecieron a finales del siglo pasado y lograron obtener cierto reconocimiento legal (*cfr.* art. 11 Tratado de la OMPI sobre Derecho de Autor de 1996). Posteriormente, destaca en el área de la protección de datos personales el movimiento del *privacy by design* (5) . Más recientemente destacan los protocolos *blockchain* (6) , éstos últimos llamados a tener en el futuro un papel disruptivo en la regulación de transacciones o relaciones electrónicas de todo tipo.

III. ALGUNOS MEDIOS DE TUTELA LEGAL DE RECURSOS INMATERIALES EN IoT

Las actividades y sectores potencialmente amparados bajo el paraguas del IoT / *Big Data* son de una amplísima diversidad y vocación multi-sectorial: medios de transporte, educación e investigación, sanidad, logística, producción industrial y robótica, gestión urbana, servicios medioambientales, energía, seguridad pública, medios de comunicación y contenidos, por citar algunas. En un contexto tan heterogéneo, diversas ramas de nuestro ordenamiento serán relevantes. Con todo, indudablemente los recursos inmateriales serán objeto de especial interés en este entorno. Veamos a continuación de forma sucinta algunos medios de tutela que en mi opinión están llamados a tener un papel destacado en este ámbito.

1. La regulación contractual

El medio de tutela legal o gobernanza más frecuente en IoT / *Big Data* es, y muy probablemente vaya a serlo por largo tiempo, la regulación contractual. Contamos con bastantes años de experiencia en relación con contratos de prestación de servicios de tecnologías de la información y comercio electrónico. Asimismo, el llamado *cloud computing*, como metáfora de Internet, ha desarrollado modelos contractuales como *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS).

En los entornos de IoT / *Big Data*, la regulación contractual sigue siendo el mecanismo más empleado para proteger y regular bienes inmateriales. Empiezan a ser frecuentes (sin duda en los EE.UU. y en UK) los contratos en los que una parte proclama su derecho de propiedad sobre datos e información (no protegibles bajo derechos de propiedad intelectual). Bajo dicha premisa, el propietario de tales datos e información impone restricciones a su contraparte contractual, justificadas en su pretendido dominio de los datos que cede de forma temporal, normalmente para la prestación de un servicio de tratamiento de información, de media o larga duración.

La Comisión Europea, en su iniciativa de fomento de una economía digital, ha identificado la tendencia a restringir la

circulación de los datos e información (no personales) mediante restricciones contractuales. En este sentido, se están considerando posibles alternativas, como soluciones inspiradas en el sistema de cláusulas abusivas aplicable en relaciones B2C, o modelos estándar de cláusulas recomendadas, con el fin de desincentivar las restricciones al libre acceso a datos. Incluso se consideran sistemas de acceso obligatorio en términos FRAND a cambio de remuneración. La reciente Ley *Lemaire* francesa (LOI n.º 2016-1321 de 7-X-2016) impone ciertas obligaciones de concesión de acceso a determinados tipos de datos. La dificultad de consensuar un marco general común probablemente impulse iniciativas desde sectores empresariales concretos [ver, por ejemplo, en el sector de la automoción: ACEA Position Paper: Access to vehicle data for third-party services de diciembre 2016 (7)].

Por otro lado, respecto a los denominados «smart contracts» (8) basados en protocolos *blockchain*, los retos de gobernanza son aún mayores, al constatar una suerte de fusión entre la propia prestación contractual y las supuestas reglas que la deben gobernar.

2. Secretos industriales

Aquellos recursos inmateriales que puedan preservarse en el entorno interno del prestador de servicios, o que se compartan de forma controlada bajo restricciones contractuales de confidencialidad, podrán valerse de esta forma de protección. La reciente Directiva 2016/943 de secretos comerciales establece ciertas condiciones para su protección: (i) carácter secreto, es decir, su poseedor o titular no sólo no ha divulgado una información objeto de protección, sino que ha impedido su conocimiento o acceso público. Si una información es generalmente conocida, o fácilmente accesible, probablemente no será considerada como merecedora de protección; (ii) valor industrial o comercial, en dos vertientes: (a) cierto mínimo nivel cualitativo de la información o conocimiento considerados en sí mismos, y (b) asignación de valor por su carácter secreto, y (iii) esfuerzo de preservación en secreto. La información o conocimientos en cuestión han de haber sido objeto de medidas razonables para preservar su carácter secreto.

Es cada vez más frecuente la aplicación del régimen legal de secretos industriales a recursos inmateriales en entornos IoT / *Big Data*. El recurso inmaterial secreto puede ir desde el propio método o sistema gestionado en un entorno de IoT hasta los propios datos e información. Respecto a estos últimos, en general considero deseable impedir una aplicación expansiva del concepto de secreto industrial a los datos e información en sí mismos por motivos diversos: generación de datos por terceras partes independientes al poseedor de los mismos, carácter trivial de los mismos, freno al intercambio y acceso público a información, etc.

3. La protección mediante patentes

Sin duda muchos participantes en entornos de IoT y *Big Data* considerarán que aspectos de sus iniciativas empresariales son materia potencialmente patentable. Entiendo que una de las cuestiones que más se suscitarán en este ámbito se refiere al debate sobre la patentabilidad de invenciones implementadas por programas de ordenador.

La EPO (Oficina Europea de Patentes) ha tratado de elaborar normas claras y objetivas sobre patentabilidad de patentes de software. En primer lugar, cualquier software que sea patentable debe tener algún carácter técnico (9) , lo que significa que los programas «en sí mismos» que no interactúan de algún modo con el mundo físico están excluidos de patentabilidad en virtud del artículo 52 (2) y (3) EPC (*e.g.* un algoritmo en sí mismo).

La fase inicial de determinación del carácter técnico de la invención solicitada es independiente del estado de la técnica y, por lo tanto, no necesita acreditarse su novedad. En la práctica, la EPO ha flexibilizado un tanto la aplicación de este primer filtro de determinación del carácter técnico en los últimos años, por lo que un buen número de aplicaciones cuidadosamente redactadas lo pasan y entran en fase de examen de los requisitos de novedad y actividad inventiva.

En los EE.UU., diversas resoluciones de su Tribunal Supremo de los últimos siete años han alterado considerablemente la forma en que se conceden este tipo de patentes. Antes del año 2010, prácticamente todas las solicitudes de patentes implementadas por software eran patentables. Después de las sentencias en *Bilski v Kappos* (2010), *Mayo v Prometheus* (2012) y *Alice Corporation v CLS Bank* (2014) esa premisa ya no aplica y las condiciones para conceder este tipo de patentes son más exigentes y, en parte, algo alineadas con la práctica de la EPO.

La concesión y validez de patentes sobre software continuarán siendo complejas, como compleja es la línea divisoria entre un mero algoritmo y una invención altamente técnica en cuya ejecución media la utilización de software.

4. Bases de datos

Las bases de datos son susceptibles de protección (directa) en la EU por una doble vía: (i) como compilaciones de datos u obras protegidas ordenadas de manera original, alcanzando la protección a la estructura y formato de la base de datos y (ii) como un derecho de nuevo cuño o «*sui generis*» que protege la inversión del productos de la base de datos frente a extracciones o reutilizaciones sustanciales no autorizadas de los datos.

En mi opinión los tribunales españoles han sido excesivamente recelosos en la aplicación de la normativa de derechos de autor a las bases de datos de estructura original, y la regulación del derecho *sui generis* ha sido objeto de constantes cuestionamientos interpretativos en forma de cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea. No considero, por tanto, ninguno de estos sistemas de protección como verdaderamente efectivos en contextos de IoT y *Big Data*, al menos en su configuración legislativa actual.

5. Protección de la interfaz gráfica de usuario

Como es sabido, los programas de ordenador se protegen como obras de creación bajo el sistema de derechos de autor (*cfr*. arts. 10.1.i) y 95 y ss. RDL 1/1996). Las interfaces gráficas de usuario («GUIs» en abreviación inglesa) son dispositivos lógicos que facilitan la interacción entre usuario y hardware. El diseño de las GUIs de aplicaciones complejas requiere de esfuerzos para lograr su simplificación y facilidad de uso.

Según la sentencia del TJUE de 22-XII-2010 (caso C-393/09), la interfaz gráfica de los programas de ordenador está excluida de la protección específica como programa de ordenador al no permitir reproducir el programa. No obstante, el TJUE confirmó que la interfaz puede merecer una protección independiente como una obra protegida por derechos de autor siempre que cumpla los requisitos generales de originalidad. La sentencia además excluyó la concurrencia de originalidad en aquellos componentes de la GUI que únicamente se caractericen por su función técnica, en aplicación de la doctrina de la fusión idea/expresión.

6. Protección de datos personales

Muchas actividades de IoT / *Big Data* comportan el tratamiento de datos de carácter personal (cuyo perímetro definitorio se ha ido incrementando con el paso del tiempo). El volumen, intensidad y variedad de propósitos del tratamiento plantean la cuestión de si el marco normativo actual es el apropiado. En todo caso, la normativa más actual (GDPR) ya acomete diversos aspectos relacionados con este tipo de tratamientos. Para muchos, los operadores de IoT / *Bid Data* deberán ganarse la confianza de sus potenciales usuarios respecto al tratamiento de sus datos, y el cumplimiento con la normativa será una de las formas de conseguirlo (10) .

IV. LA (RE)CONFIGURACIÓN DE LOS DERECHOS IP EN ENTORNOS DE IoT / BIG DATA

Los nuevos escenarios de IoT / *Big Data* se caracterizan por el dinamismo y velocidad en los procesos de generación de datos e información.

Así, nos movemos en relaciones de prestación de servicios con más elementos que una mera venta de un bien concreto. Pongamos un ejemplo: alquiler de un sistema de hardware equipado con sensores que obtiene datos sobre rendimiento de una infraestructura productiva, viniendo dicho hardware acompañado de un software analítico que permite al usuario gestionar la planta de producción de forma más eficiente y recibiendo el usuario del sistema servicios de valor añadido relacionados, por ejemplo, con el mantenimiento preventivo de la maquinaria analizada o el estudio de los datos recabados con el fin de lograr futuras mejoras en productividad. El potencial de este tipo de soluciones abarca muchos sectores (*retail*, automoción, energía, etc.), siendo ya realidad en muchos de ellos.

Tanto el IoT, como los análisis de *Big Data*, precisamente descansan sobre dichos recursos info-analíticos en entornos, como hemos visto, de gran volumen, de disparidad del origen de los datos y de gran fluidez del tratamiento. Ello nos lleva a destacar una característica muy relevante de la gestión de recursos inmateriales en escenarios de IoT y *Big Data*: su naturaleza prestacional propia de una relación de servicios; ello nos alejaría de los tradicionales ámbitos patrimoniales o demaniales, de naturaleza estática, más propios de modelos de negocio que se limitan a comercializar activos concretos. En este contexto **¿llegará a consolidarse un *IP as a service* (IPaaS)?**

Nuestro país, con un gran volumen de dispositivos conectados *on-line* (11) **, la red de fibra óptica más extensa de Europa y con excelentes profesionales de las TIC, está en buenas condiciones para aprovechar el IoT y *Big Data* como factores de innovación y generación de oportunidades empresariales.**

(1) K. SCHWAB, The Fourth Industrial Revolution: what it means, how to respond, (14-I-2016), https://www.weforum.org/agenda/2016/01/the-fourth-

industrial-revolution-what-it-means-and-how-to-respond (último acceso 23-V-2017).

(2) V. ELAM, CAD Files and European Design Law, JIPITEC 7 (2) 2016 accesible en http://www.jipitec.eu/issues/jipitec-7-2-2016/4439 (último acceso 23-V-2017).

(3) «Raw machine-generated data are not protected by existing intellectual property rights since they are deemed not to be the result of an intellectual effort and/or have any degree of originality.» Comunicación de la Comisión Europea «Building a European data economy», Bruselas 10-I-2017 - com (2017) 9 final.

(4) Sobre esta cuestión véase nuestro trabajo S. Miralles, Titularidad de datos e información en entornos de datos masivos (Big Data), libro conmemorativo del 50 Aniversario del Grupo Español de la AIPPI, abril 2015 (original entregado en abril de 2014).

(5) Impulsado inicialmente por la responsable de protección de datos de la provincia canadiense de Ontario, ver https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/ y respecto a su recepción en la EU puede consultarse https://www.enisa.europa.eu/topics/data-protection/privacy-by-design (últimos accesos 23-V-2017).

(6) K. BHEEMAIAH, Blockchain 2.0: the renaissance of money, accesible en https://www.wired.com/insights/2015/01/block-chain-2-0/ (último acceso 23-V-2017).

(7) Accesible en «http://www.acea.be/publications/article/position-paper-access-to-vehicle-data-for-third-party-services» (último acceso 23-V-2017).

(8) Los contratos inteligentes o «smart contracts» son líneas de código informático incrustadas en el protocolo blockchain que describen una serie de obligaciones y permiten su ejecución automática cuando se cumplen las condiciones en ellas descritas. En su esencia son inmutables y, por tanto, las consecuencias de su ejecución son irreversibles.

(9) La decisión de Sala de Recurso de la EPO T 1173/97 (IBM) de 1-7-1988 estableció: «A computer program product is not excluded from patentability under Article 52 (2) and (3) EPC if, when it is run on a computer, it produces a further technical effect which goes beyond the "normal" physical interactions between program (software) and computer (hardware)». Ver también decisión T 0154/04 (Duns L. Ass.) de 15-11-2006.

(10) INFORMATION COMMISSIONER OFFICE (UK), Big data, artificial intelligence, machine learning and data protection. 20170301. Version: 2.0.

(11) OECD Digital Economy Outlook 2015, pág. 261 accesible en http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#.WM5f2vk1-yI#page261 (último acceso 8-V-2017).