



## Trabajo Fin de Grado

Internet de las Cosas: propiedad de los datos y su  
tratamiento como secretos empresariales

*Internet of Things: data ownership and data  
protection as trade secrets*

Autora

María Janeta Stroe

Director

Pedro José Bueso Guillén

Facultad de Derecho  
2019/2020

**RESUMEN:** El presente trabajo analiza los aspectos legales derivados de la evolución del Internet de las cosas en las empresas y la creciente implementación de la Industria 4.0. Es por ello, que cada vez más empresas persiguen la incorporación de soluciones tecnológicas en sus productos y servicios, como son los sensores, la inteligencia artificial y el Big data. El objetivo de este estudio es conocer la regulación actual sobre la protección que se les concede a las empresas que apuestan por obtener una ventaja competitiva a partir de la recopilación de datos no personales gracias a dispositivos o maquinarias, exponiendo las carencias y soluciones de la normativa europea y nacional en esta materia.

**ABSTRACT:** This essay analyzes the legal aspects derived from the evolution of the Internet of Things in companies and the increasing implementation of the Industry 4.0. That is why, more and more companies are supporting the incorporation of technological solutions in their products and services, such as sensors, artificial intelligence and Big Data. The objective of this study is to know the current regulation on the protection granted to companies that choose to achieve a competitive advantage from the collection of non-personal data through devices or machines, exposing the deficiencies and solutions of European and national regulation on this subject.

## ÍNDICE

<b>I. INTRODUCCIÓN</b>	<b>5</b>
<b>1. TEMA OBJETO DE ANÁLISIS DEL TRABAJO</b>	<b>5</b>
<b>2. RAZÓN DE ELECCIÓN DEL TEMA</b>	<b>6</b>
<b>3. METODOLOGÍA SEGUIDA EN EL DESARROLLO</b>	<b>6</b>
<b>II. ANÁLISIS DE CASO CONCRETO: CONER</b>	<b>8</b>
<b>1. DESCRIPCIÓN DE LOS HECHOS Y CIRCUNSTANCIAS</b>	<b>8</b>
<b>2. CUESTIONES JURÍDICAS QUE SE PLANTEAN</b>	<b>9</b>
<b>3. NORMATIVA APLICABLE</b>	<b>10</b>
<b>4. FUNDAMENTOS DE DERECHO</b>	<b>11</b>
4.1. ANÁLISIS DE LOS DATOS RECOPIADOS POR CONER: DATOS PERSONALES O NO PERSONALES.	11
4.2. PROPIEDAD DE LOS DATOS	16
A) <i>Conceptos y planteamiento de la cuestión de la propiedad de los datos</i>	16
B) <i>Las opciones tratadas en el ámbito de la propiedad</i>	21
<b>5. CONCLUSIONES SOBRE EL DICTAMEN</b>	<b>28</b>
5.1. SOLUCIONES BASADAS EN LA TITULARIDAD DE LOS DATOS DE CONER	28
5.2. SOLUCIONES BASADAS EN LA PROTECCIÓN DE LOS DATOS DE CONER COMO SECRETO EMPRESARIAL	30
<b>III. CONCLUSIONES FINALES</b>	<b>33</b>
<b>IV. BIBLIOGRAFÍA</b>	<b>35</b>
A) FUENTES DOCTRINALES	35
B) DOCUMENTOS LEGISLATIVOS Y PROPUESTAS	37
C) FUENTES JURISPRUDENCIALES	38
D) CONSULTAS ARTÍCULOS Y PÁGINAS DE INTERNET	39

## ABREVIATURAS

**AEPD:** Agencia Española de Protección de Datos.

**Art.:** Artículo.

**CC:** Código Civil.

**GATT:** Acuerdo General sobre Aranceles Aduaneros y Comercio.

**IoT/IoC:** *Internet of Things* o Internet de las cosas.

**IIoT:** *Industrial Internet of Things* o Internet Industrial de las cosas.

**ITAINNOVA:** Instituto Tecnológico de Aragón

**LOPD:** Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (anteriormente vigente)

**LOPDGDD:** Ley orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

**LSE:** Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

**OMC:** Organización Mundial del Comercio.

**OMPI:** Organización Mundial de la Propiedad Intelectual (en inglés *WIPO*)

**PI:** Propiedad intelectual.

**RGPD:** Reglamento General de Protección de Datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016).

**TFUE:** Tratado de Funcionamiento de la Unión Europea.

**TJUE:** Tribunal de Justicia de la Unión Europea.

**TS:** Tribunal Supremo

**UE:** Unión Europea.

## I. INTRODUCCIÓN

### 1. TEMA OBJETO DE ANÁLISIS DEL TRABAJO

En los últimos años, debido al impulso de las diferentes tendencias tecnológicas relacionadas con el ámbito de la economía digital, entre muchas otras, el Internet de las cosas (*IoT*), el aprendizaje automático, la inteligencia de datos, la inteligencia artificial y la computación en la nube, se ha generado un gran interés hacia los datos obtenidos por estos mecanismos.

Además, hay que tener en cuenta que las tecnologías de la información no sólo afectan a los individuos como ciudadanos, sino que de una forma avanzada empiezan a adentrarse en el mundo empresarial, siendo, sobre todo, de gran aplicación e importancia dentro del sector industrial, dando lugar a lo que se conoce como *Industria 4.0*, sumando en sus actividades múltiples tecnologías: sensores, IIoT, analítica y *big data*...

Es por ello que el tema sobre el que versará este trabajo es el de la influencia que la implantación de la tecnología en el sector industrial -sus productos y servicios- ha tenido sobre el Derecho, en concreto, sobre la aplicabilidad de una normativa cambiante y los problemas legales que surgen en este ámbito. Para ello, este trabajo de fin de grado se fundamenta principalmente en el análisis de un caso práctico -en forma análoga al dictamen- de los problemas jurídicos que se plantean en el proyecto que la empresa española líder en la creación de maquinaria ligera de construcción CONER<sup>1</sup> está actualmente desarrollando junto con el Instituto Tecnológico de Aragón, de ahora en adelante, ITAINNOVA.

Dicho proyecto consiste en la implantación de sensores en los productos que CONER fabrica para poder recolectar datos provenientes de los mismos, y ello con el fin de poder generar nuevos conocimientos para diseñar productos futuros. De este modo, el análisis de los datos obtenidos mediante un elemento puramente tecnológico puede generar tanto una importante ventaja competitiva para las empresas como suscitar dudas desde una perspectiva jurídica.

---

<sup>1</sup> Nombre ficticio para preservar la confidencialidad de los datos de la empresa.

## 2. RAZÓN DE ELECCIÓN DEL TEMA

El tema elegido está relacionado en su gran mayoría con temas de gran actualidad en el mundo empresarial y legal actual, siendo esta razón un gran atractivo a la hora de desarrollar este Trabajo de Fin de Grado frente a otros temas propuestos.

Los datos se han convertido en el recurso esencial para el crecimiento empresarial y desarrollo social. Por tanto, la innovación, la optimización y análisis de los datos es una tendencia fundamental a la hora de integrarlo dentro de todos los sectores de la economía.

Por otra parte, la tendencia legislativa en materia de protección de datos y la todavía poca experiencia en el sector de *Legaltech*, así como la escasa normativa en este ámbito, hace aún más sugerente este tema de cara a analizarlo en mi trabajo.

Por último, el hecho de tener la oportunidad de realizar el trabajo sobre un caso real, y tener la posibilidad de que toda la información recopilada y las posibles soluciones a las que llegue pueda servir de aplicación por la empresa CONER. Además, de poder englobarse el trabajo dentro del marco de la colaboración que se está llevando a cabo entre ITAINNOVA y el Grupo de Investigación LegMiBIO, al cual pertenece el profesor Pedro Bueso Guillén, director de este trabajo.

## 3. METODOLOGÍA SEGUIDA EN EL DESARROLLO

Para la realización de dicho trabajo se ha seguido una metodología de investigación científica, para poder analizar las cuestiones jurídicas que plantea un problema real y dar las pertinentes conclusiones.

En concreto, el procedimiento metodológico seguido se ha basado en un pluralismo de técnicas y métodos, basándome principalmente en una investigación analítica y deductiva al descomponer un problema complejo en sus diferentes elementos para analizarlos individualmente aplicando las disciplinas del derecho y la interpretación de normas jurídicas. También, se han utilizado en el desarrollo del trabajo una investigación documental intentando que sea tanto de información primaria -normas jurídicas- como secundaria- estudio del derecho a través de la doctrina y/o jurisprudencia.

Aplicando la metodología descrita, para el desarrollo de esta investigación, el trabajo realizado se han dividido en las siguientes fases:

- Elección del tema y concreción del objeto de la investigación, mediante una entrevista con CONER e ITAINNOVA, seguida de diversos intercambios de información por correo electrónico.
- Documentación y búsqueda de información sobre el Derecho positivo aplicable al caso, tanto en bases de datos de normativa, como de doctrina y de instituciones (como la AEPD).
- Análisis e interpretación del material y aplicación a los elementos del problema.
- Redacción del trabajo, concluyendo con una solución al problema, y posterior lectura para fijar la versión final del mismo.

## II. ANÁLISIS DE CASO CONCRETO: CONER

### 1. DESCRIPCIÓN DE LOS HECHOS Y CIRCUNSTANCIAS

La empresa CONER, como ya se ha mencionado, líder en la fabricación de maquinaria ligera para la construcción que opera en más de 134 países, tales como México, Francia, y China, tiene por actividad comercial habitual la venta de productos maquinaria ligera de construcción, productos que vende a compradores principalmente de la zona comunitaria para que utilicen el producto para uso propio o para su posterior reventa o alquiler a clientes finales. Su maquinaria está distribuida mediante diferentes canales de distribución en función del mercado geográfico al que se quiere alcanzar.

Por ello, en el ámbito de interés de países fuera de la UE, como por ejemplo Estados Unidos y Canadá, la principal metodología es la distribución en exclusiva del producto o familia de los productos mediante un *importador*. En definitiva, ambas situaciones conceden la propiedad de la máquina al comprador o importador al realizarse la compraventa, transmitiéndose dicha propiedad en el momento de la expedición a través de factura comercial, sea en España, Europa o cualquier otra parte del mundo donde se distribuya.

Recientemente, la empresa junto con ITAINNOVA, ha decidido fomentar el desarrollo de un nuevo sistema de innovación mediante la incorporación de sensores en las máquinas para poder recopilar información que tenga como única función la posterior mejora de los productos.

Estos sensores incorporados en las máquinas captarán directamente la información, sin ser necesario que el distribuidor ni el cliente final tengan que realizar alguna acción, recopilada en la sede de la empresa mediante un sistema de *Cloud Computing* para posteriormente analizar los datos y mejorar sus productos.

Cabe recordar, que por IoT nos referimos a toda conexión de un objeto a Internet mediante sensores que envían y reciben datos, y más específicamente la IIoT supone que estos sistemas estén implementados dentro de la industria, beneficiándose las empresas del uso de los datos para una mejora gestión de sus recursos o de una mejor producción de sus productos.



Por todo ello, es imprescindible enumerar los datos que se van a recopilar y sobre los que posteriormente se va a trabajar:

- a) Fecha del primer uso de la máquina.
- b) Número de horas de trabajo total: principalmente para recopilar las horas de vida trabajadas acumuladas del equipo.
- c) Ciclos de uso: referidos al tiempo de trabajo desde que se pone en marcha la máquina hasta que se apague.
- d) Averías y mantenimiento realizado.
- e) Actualización de software.
- f) Bloqueo de la máquina.
- g) Modificación de parámetros técnicos.
- h) Localización geográfica o ubicación del equipo.

## 2. CUESTIONES JURÍDICAS QUE SE PLANTEAN

En definitiva, debido a este nuevo proyecto se han planteado una serie de cuestiones jurídicas que se van a desarrollar a través de este trabajo. Podemos diferenciar por tanto los siguientes problemas a los que se deben hacer frente:

- a) Se debe analizar si los datos recopilados por CONER mediante los sensores se pueden considerar datos personales o no para conocer si es aplicable al caso la normativa de protección de datos personales.
- b) Sobre la distinción entre datos personales y datos no personales, se debe esclarecer la cuestión de la propiedad de los datos generados por la máquina, y saber quién o quiénes de todos los sujetos sucesivos del canal de distribución son los que poseen el derecho de propiedad sobre los mismos.
- c) Y consecuentemente, plantear formas de asignar la propiedad de los datos a la empresa y proteger a CONER de posibles acciones de terceros que impidan o dificulten la recogida de estos datos, si fuera preciso, mediante posibles cláusulas contractuales.

### 3. NORMATIVA APLICABLE

Para la resolución de las cuestiones jurídicas planteadas es de posible aplicación la siguiente normativa:

- Código Civil Español.
- 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 (en adelante, RGPD).<sup>2</sup>
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD)<sup>3</sup>.
- Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (en adelante, Reglamento (UE) 2018/1807)<sup>4</sup>
- Directiva (UE) 2016/943 de 8 junio de 2016 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.<sup>5</sup> (en adelante, Directiva de Secretos Comerciales).
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales (en adelante, LSE).<sup>6</sup>

---

<sup>2</sup> Diario Oficial de la Unión Europea L 119/1 de 4 de mayo de 2016 EUR-Lex: <http://data.europa.eu/eli/reg/2016/679/2016-05-04>

<sup>3</sup> BOE núm. 294, de 6 de diciembre de 2018 (BOE-A-2018-16673). Recuperado de: <https://www.boe.es/eli/es/lo/2018/12/05/3/con>

<sup>4</sup> Diario Oficial de la Unión Europea. L 303 de 28.11.2018. EURLEX: <http://data.europa.eu/eli/reg/2018/1807/oj>

<sup>5</sup> Diario Oficial de la Unión Europea L 157/1 de 15.06.2016 EURLEX: <http://data.europa.eu/eli/dir/2016/943/oj>

<sup>6</sup> BOE núm. 45 de 21 de febrero de 2019 (BOE-A-2019-2364). Recuperado de: <https://www.boe.es/eli/es/l/2019/02/20/1/con>

## 4. FUNDAMENTOS DE DERECHO

### 4.1. Análisis de los datos recopilados por CONER: datos personales o no personales.

Según la Comunicación de la Comisión sobre “La Construcción de una Economía de los Datos Europea”<sup>7</sup>, los datos generados por las máquinas sin intervención humana directa, a través de aplicaciones o sensores que procesan estos datos, pueden ser personales o no personales, dependiendo de si pueden o no identificar a una persona o incluso de si han sido totalmente anonimizados (en el caso de que sean personales).

Además, como menciona el Considerando 9 del Reglamento (UE) 2018/1807 se incluyen, entre las fuentes de datos no personales, el Internet de las cosas; pero, no obstante, se debe examinar caso por caso para averiguar si estos datos pueden o no considerarse datos personales.

Son datos personales «toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (art. 4 RGPD).

A considerar «toda información», estamos ante un concepto amplio, ya que su concreción depende de la evolución de la sociedad y la tecnología. Por consiguiente, comprende tanto a la información objetiva como a la subjetiva; así, un elemento genético (sangre) sería una información objetiva mientras que datos financieros y bancarios serían considerados como una información subjetiva (por ejemplo: “X es prestatario”). Además, no es relevante ni necesario que la información esté recogida en una base de datos, cabiendo la información desestructurada y en cualquier formato o soporte.<sup>8</sup>

Por último, también hay que hacer una breve mención sobre la referencia a la terminología «persona identificada o identificable», ya que, a primera vista, la información puede no identificar a la persona, pero posteriormente, mediante una combinación de datos obtenidos, sí que podría distinguir a la correspondiente persona.

---

<sup>7</sup> Comisión Europea. “Comisión Europea. *Building a European Data Economy*. [La Construcción de una Economía de los Datos Europea], Comunicación, COM (2017) 9 final, 10 de enero 2017. Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017DC0009>

<sup>8</sup> GRUPO DE TRABAJO DEL ARTÍCULO 29, “Opinion 4/2007 on the Concept of Personal Data” (2007). WP 136 del 20 de junio de 2006.

Por ello, hay que tener en cuenta que la posibilidad de identificación de una determinada persona no sólo es el conocimiento de sus nombres y apellidos, sino que se puede identificar al usuario uniendo diferentes piezas atribuibles a su posible personalidad (un ejemplo sería la utilización de cookies).<sup>9</sup>

La protección de los datos merece el reconocimiento de derecho fundamental recogido en el art. 16 del TFUE, y en el art. 8 de la Carta de Derechos Fundamentales de la UE. Debido a este reconocimiento esencial, la Unión Europea reguló la protección de los datos personales desde el año 1995 mediante la Directiva 95/46/CE, que posteriormente ha sido sustituida en el año 2016 por el RGDP.

En cuanto al ámbito nacional, la protección de datos personales está regulada en la vigente LOPDGDD, que viene a complementar el RGPD y ha venido a derogar a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal<sup>10</sup> (en adelante, LOPD).

En principio, ninguno de los datos que son recabados en este caso parece conducir a poder identificar directa o indirectamente a una persona tal y como requiere el RGPD, ya que sólo estamos haciendo referencia a datos concretos de la máquina (fecha del primer uso, número horas acumuladas de trabajo, ciclo de uso de la máquina, averías y mantenimiento realizado, actualización de software, bloqueo de la máquina, modificación de parámetros técnicos y ubicación).

Tal y como se establece en el Considerando 9 del Reglamento (UE) 2018/1807 «entre los ejemplos específicos de datos no personales se encuentran [...] los datos sobre las necesidades de mantenimiento de máquinas industriales. Si los avances tecnológicos hiciesen posible transformar datos anónimos en datos personales, dichos datos se deben tratar como datos personales y, en consecuencia, se debe aplicar el Reglamento (UE) 2016/679». Estos datos se recolectan para mejorar la máquina y con el interés de establecer qué necesidades pueden tener según su uso y así, mejorar sus características y atributos, por lo que, consecuentemente, se puede incorporar en lo que establece este considerando como “necesidades de mantenimiento de máquinas industriales”.

---

<sup>9</sup> *Ibidem*.

<sup>10</sup> BOE núm. 298, de 14 de diciembre de 1999 (BOE-A-1999-23750). Recuperado de: <https://www.boe.es/eli/es/lo/1999/12/13/15/con>

El único dato que podría plantear problemas en cuanto a su posibilidad de considerarse un dato personal es la localización o ubicación, ya que los datos de localización han sido definidos según el art. 2 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)<sup>11</sup> como «cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público».

A pesar de que la actual propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónica<sup>12</sup>, que sustituiría a la vigente Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas anteriormente mencionada<sup>13</sup>, no recoge esta definición, la AEPD sigue entendiendo el dato de localización conforme a la anterior definición, además de lo establecido en el art. 64.b) del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios<sup>14</sup> que cita, a efectos de dicho título, que los datos de localización se entienden por «cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público».

En consecuencia, la AEPD ha indicado que los datos de localización serán siempre considerados como un dato personal en cuanto se refieran a una persona física identificada o identificable, en virtud del RGPD.<sup>15</sup>

---

<sup>11</sup> Diario Oficial de la Unión Europea L 201 de 31 de julio de 2002. EUR-Lex: <http://data.europa.eu/eli/dir/2002/58/2009-12-19>

<sup>12</sup>DOUE: COM/2017/010 final – 2017/03 (COD) EUR-Lex: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0010>

<sup>13</sup> *Op cit.* (Supra 10, pág. 11).

<sup>14</sup> BOE núm. 102, de 29 de abril de 2005 (BOE-A-2005-6970). Recuperado de: <https://www.boe.es/eli/es/rd/2005/04/15/424/con>

<sup>15</sup> Así lo han reflejado múltiples resoluciones de la AEPD como por ejemplo la E/00827/2018 y E/00868/2018.

En este caso, hay que decir que el dato que se recoge por la empresa es la localización de la máquina en sí, no localizando por tanto a ninguna persona física ya que, la maquinaria puede estar dentro del almacén de la empresa compradora o en las instalaciones en las que los trabajadores de esta empresa desarrollen su trabajo. No existiendo de tal manera ningún fin de localización de una persona física concreta.

Por consiguiente, como esta localización lo que nos permitirá ubicar es a la máquina y consecuentemente a la empresa propietaria de la misma o las instalaciones en las que desarrolla su actividad, de la cual CONER ya es conocedora de su identidad por haberse realizado un contrato de compraventa o arrendamiento, no se podrá considerar a este dato como un dato personal.

Adicionalmente, se señala que expresamente en el considerando 14 del RGPD su ámbito de aplicación subjetivo *«La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a las personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto»*, no comprendiendo a los supuestos en que dichos datos personales se recopilen sobre las personas jurídicas.

Por consiguiente, para las situaciones dónde el cliente sea una persona jurídica, que será la mayoría de los casos, no existirá ningún problema sobre este datos de localización al no ser de aplicación el RGPD ni la LOPDGDD.

Aun con ello, se debe dejar claro que la intención de la empresa no es en ningún caso analizar la información recabada para incidir en la vida privada de las personas físicas. Y, aunque pueda ser probable que este procedimiento recopile ciertos datos asociables al personal encargado de las máquinas, dicha recopilación sólo sería con el fin de obtener un *feedback* (sugerencias y consultas para los compradores). De ahí que, ante esta situación, pueda ampararse en la presunción del art. 19 de la LOPDGDD en relación con el art. 6.1 f) del RGPD estableciendo estos datos como «datos profesionales».

Este término implica la posibilidad de realizar un tratamiento lícito de los datos sin necesidad de recabar el consentimiento. En este sentido, se debe señalar la jurisprudencia

reiterada del TJUE<sup>16</sup>, donde establece que las excepciones y restricciones a la protección de datos personales han de establecerse sin sobrepasar los límites de lo estrictamente necesario.

También, resulta oportuno atender al Considerando 47 del RGPD, que literalmente afirma que «existirá un interés legítimo por parte de un responsable de tratamiento [...] siempre y cuando no prevalezcan los intereses o los derechos y libertades del interesado [...]. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable».

Aun así, cabe mencionar que si los datos fuesen sobre una persona física, como lo serían los empleados, para poder evitar posibles futuros problemas en la medida en que se puedan considerar datos personales, es recomendable proceder a una anonimización de los mismos. Entendiendo por «anonimización» según la AEPD como la ruptura de la cadena de identificación de las personas, existiendo múltiples técnicas para ello, entre las cuales podemos destacar, por ejemplo; enmascarar los datos, la pseudoanonimización, los algoritmos, el cifrado de datos, etc. De esta manera, tal y como se establece en el Considerando 26 del RGPD, se entenderá que una vez anonimizados los datos, ya no se les aplicaría la normativa de protección de datos.<sup>17</sup>

Adicionalmente, puede suceder que el problema no sea principalmente del tipo de datos recopilados, sino de la cesión o no de los mismos a los clientes de la empresa para su uso. Y, para evitar un posible cruce de datos que existiría ante un derecho de cesión de los datos recopilados, es necesario recomendar que la empresa asegure su única utilización a través de cláusulas contractuales de confidencialidad evitando el uso y acceso por sus clientes y por terceros a estos datos.

---

<sup>16</sup> Sentencia del TJUE (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland Ltd*, asuntos acumulados C-293/12 y C-594/12, EU:C:2014:238 apartado 52, Recuperado en: <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62012CJ0293> ; Sentencia del TJUE (Sala Tercera) de 7 de noviembre de 2013, *IPI vs Englebert*, C-473/12, EU:C:2013:715, apartado 39 y resto de jurisprudencia citada, Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0473>

<sup>17</sup> Según se establece en el Considerando 26 del RGPD «los principios de protección de datos no deben aplicarse a la información anónima, es decir, información que no guarda relación con ninguna persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo».

## 4.2. Propiedad de los datos

### A) Conceptos y planteamiento de la cuestión de la propiedad de los datos

Los datos y la información que contienen se han convertido en la actualidad en los activos intangibles<sup>18</sup> más importantes en el sector empresarial<sup>19</sup> al incorporar algún tipo de conocimiento a las industrias y empresas, al mismo tiempo que servir como una mercancía intercambiable por un valor monetario, ya sea información personal o no.<sup>20</sup>

La evolución de la economía digital nos ha ido dejando múltiples nuevos conceptos jurídicos e interpretaciones de estos, y no es menos decir que la revolución digital ha creado -simplificando- dos nuevos conceptos: los bienes informáticos/digitales y los bienes informacionales (los datos).<sup>21</sup> Dicho de otro modo, los bienes digitales son todos aquellos que se encuentran en el ciberespacio, mientras que los datos, entendidos como bienes informacionales, se han convertido en objetos de cambio intangibles y consecuentemente en bienes en sentido jurídico-patrimonial.<sup>22</sup>

La propiedad de un bien inmaterial no se puede equiparar enteramente al derecho de propiedad de un bien material, como lo es por ejemplo una máquina o un libro, donde se obtiene el uso, disfrute y posesión.<sup>23</sup> En cambio, en los bienes intangibles caben ciertas

---

<sup>18</sup> Los bienes intangibles se pueden definir como aquellos que no pueden apreciarse por los sentidos, al tratarse de cosas inmateriales, pero esta definición desde un punto de vista negativo no puede ser válida en sentido técnico jurídico. Para Díez-Picazo, los bienes inmateriales «son las realidades, que careciendo de existencia corporal y siendo un producto o creación intelectual del espíritu, el ordenamiento jurídico valora como posible objeto de derecho subjetivos» [DÍEZ-PICAZO, L. *Fundamentos del derecho civil patrimonial. Las relaciones jurídico-reales. El registro de la propiedad. La posesión*. Civitas, t. III, 5ª ed., Madrid, 1996, p.159.]

<sup>19</sup> Según el informe de WORLD ECONOMIC FORUM, *Personal data: the emergence of a new asset class* (2011). Disponible en: <https://www.weforum.org/reports/personal-data-emergence-new-asset-class>

<sup>20</sup> Los datos digitales son un nuevo tipo de materia prima de la economía del siglo, siendo uno de las principales monedas de intercambio del futuro, creando a su vez nuevos modelos de mercado donde el valor de los datos será su capacidad de ser agregados. Según BAZARRA, I. “Los datos, la materia prima del siglo XXI”, Tendencias KPMG, 2019 [consultado el 14 junio 2020] Disponible en: <https://www.tendencias.kpmg.es/claves-decada-2020-2030/datos-privacidad-monetizacion/>

<sup>21</sup> CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. «Capítulo 8: Economía digital y datos entendidos como bienes», Recuperado en: <https://www.researchgate.net/publication/339363181>

<sup>22</sup> CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. «Capítulo 8: Economía digital y datos entendidos como bienes», p. 293 con cita de: Comisión Europea, Staff Working Document, “*On the free flow of data and emerging issues of the European data economy, accompanying COM (2017) 9 final*”. SWD (2017), 2 final. EUR-LEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0002>; BECKER, M. *Reconciling Data Privacy and Trade in Data – A right to Data-avoiding Products*. En *Zeitschrift Für Geistiges Eigentum – Intellectual Property Journal* 3 Band 9, 2017; ZECH, H. *Building a European Data Economy – The European Commission’s Proposal for a Data Producer’s Right*, *Intellectual Property Journal* vol. 9, pp. 317-330, 2017.

<sup>23</sup> Pero existen autores como Heverly, R. A. en *The information semicommons*, *Berkeley Technology Law Journal*, 18(4), 2003 pp. 1128-1189. sostiene que para determinar si los datos o información son propiedad



notas más peculiares; por ejemplo, la posibilidad de que la posesión del objeto sea diferente a la propiedad o titularidad del mismo, que es lo que sucede más frecuentemente en el ámbito del IoT.<sup>24</sup>

En la normativa española, el derecho de propiedad aparece regulado en el artículo 348 CC -derivado del concepto del Derecho romano- y dice : «La propiedad es el derecho de gozar y disponer de una cosa, sin más limitaciones que las establecidas en las leyes. El propietario tiene acción contra el tenedor y el poseedor de la cosa para reivindicarla».

Por lo tanto, la propiedad se refiere a «la posesión y responsabilidad sobre los datos. Implica tanto poder como control, y este control se deriva en acceder, crear, modificar, eliminar datos y todos los beneficios relacionados».<sup>25</sup>

Otra posible forma de avanzar prevista, es la creación de un nuevo derecho de producción de datos con el objetivo de mejorar la comerciabilidad de los datos mecanizados no personales o anónimos como un bien económico.<sup>26</sup>

Tal derecho podría ser considerado como un derecho *in rem*<sup>27</sup> y tener la posibilidad de ofrecerse un derecho exclusivo de utilizar ciertos datos, incluyendo el derecho a licenciar su uso. Esto incluiría un conjunto de derechos exigibles frente a cualquier parte

---

de una persona física o jurídica es necesarios examinar los derechos a utilizar, excluir el acceso y a transferirlo. Existiendo a su vez diferentes escuelas de pensamiento sobre este derecho privado; por una parte, el “esencialismo de una sola variable” sostiene que el derecho a excluir es suficiente para asegurar la propiedad; el “esencialismo de variables múltiples” sostienen que el derecho a excluir necesita del derecho de uso y transferencia; y, por último, el “nominalismo” presenta un concepto de propiedad *de facto* (*Soy dueño cuando tengo el control sobre el bien*).

<sup>24</sup> A este respecto consultar GÓMEZ SEGADÉ, J.A., *Los bienes inmateriales en el Anteproyecto de Ley del Código Mercantil*. En: Estudios sobre el futuro Código Mercantil, Universidad Carlos III, 2015, pp. 115-135.

<sup>25</sup> PODESTÁ, A.; CASTELLOTE, M.; CONSTANZO, B.; et al, *Dificultades de investigaciones penales en Cloud Computing, 2014*.

<sup>26</sup> Tal y como establecen los datos generados por máquinas son productos comercializables los autores ZECH, H. *European Contract Law and the Digital Single Market*, 2016, pp. 51-79; BECKE, M. Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: Büscher/Glückner/Nordemann/Osterrieth/Rengier (Eds.), *Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz*. Festschrift für Karl-Heinz Fezer zum 70. Geburtstag, p. 815; this response is not considered to be an advisable way forward by: OECD, *Maximising the Economic and Social Value of Data*, (forthcoming); KERBER, W., *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, GRUR Int 2016, p. 989; J. Drexl/ R. Hilty (et al.), *On the Current Debate on Exclusive Rights and Access Rights to Data at the European Level*, Max Planck Institute for Innovation and Competition Position Statement (16 August 2016), at p.12, D. Zimmer, *Fragwürdiges Eigentum an Daten*, Frankfurter Allgemeine Zeitung 18.11.2016, p. 16; *Plattform Industrie 4.0, Industrie 4.0 – wie das Recht Schritt hält*, Ergebnispapier, 2016, p. 22.

<sup>27</sup> Como ya se ha mencionado un derecho *in rem* (término usado dentro de los derechos de propiedad) significa que tiene aplicabilidad *erga omnes* - contra todo el mundo - independientemente de las relaciones contractuales.

independiente de las relaciones contractuales, impidiendo así el uso ulterior de los datos por terceros que no tienen derecho a utilizarlos, incluido el derecho a reclamar daños y perjuicios por el acceso y uso no autorizado de los datos.<sup>28</sup>

Alternativamente, en lugar de crear un derecho productor de datos como un derecho *in rem*, podría concebirse como un conjunto de derechos puramente defensivos<sup>29</sup>. Esta opción seguiría la elección de algunos autores como la protección dada al *know-how* en la Directiva de Secretos Comerciales. El objetivo sería mejorar el intercambio de los datos al menos de los elementos defensivos de un derecho *in rem*, es decir, la capacidad del titular de facto para demandar a terceros en caso de apropiación indebida de los datos. Así pues, este enfoque equivale a la protección de una “posesión” de facto y no al concepto de “propiedad”.<sup>30</sup>

Si un derecho del productor de los derechos tiene que ser creado como un derecho *in rem* y sólo para los derechos crudos (*raw*) -los datos no personales creados por máquinas- la asignación del derecho (es decir, definir el productor del dato) debe ser guiada a través de un análisis exhaustivo de todos los elementos relevantes para asignar tal derecho. Siendo uno de los criterios para asignar este derecho las inversiones realizadas y recursos invertidos en la creación de los correspondientes datos, que en la mayoría de los casos, se realizan por dos partes:

- El fabricante de las máquinas, herramientas o dispositivos equipados con correspondientes sensores que generen los datos, que es el que ha invertido en el desarrollo e innovación, y en la comercialización de la máquina, y los operadores económicos, que usan estas máquinas o herramientas pagan un determinado precio por la compra o arrendamiento de las mismas.
- Cuando varias personas o entidades realizan inversiones conjuntas en la recopilación de los datos a través de la correspondiente máquina, esto podría dar lugar a ciertos derechos conjuntos sobre los datos generados. Esta opción conduce

---

<sup>28</sup> Sin embargo, este derecho no sería concebible con respecto a los datos personales, ya que la protección de estos últimos es un derecho fundamental en sí mismo, en virtud del cual las personas físicas deben tener control de sus propios datos personales (cf. considerando 7 de la RGPD) Control asegurado por la normativa de datos personales que refuerza las obligaciones de los responsables del tratamiento de los datos y la protección de las personas físicas.

<sup>29</sup> KERBER, W *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, GRUR Int 2016, p. 989, apoya esta perspectiva.

<sup>30</sup> ZECH, H *Information as a tradable commodity*, European Contract Law and the Digital Single Market, 2016, pp. 51-63.

a ser casi imposible identificar a uno o varios propietarios, pudiéndose acudir a la titularidad de facto.

Dicho esto, el concepto que se utilizará en este trabajo va a ser un concepto absoluto y completo del derecho de propiedad -con efectos *erga omnes*-, coincidiendo con la interpretación realizada por la Comisión Europea en su documento de trabajo de 2017 sobre la libre circulación de datos y las cuestiones emergentes de la economía europea de datos.<sup>31</sup>

Al no existir una normativa europea que regule el concepto de «derecho de propiedad», resulta interesante realizar un inciso sobre derecho comparado de los diferentes países. En el Derecho civil la propiedad es mayormente definida e individualizada en una serie de objetos -conocidos por el nombre de *numerus clausus*-, por lo contrario en *Common Law* la regulación es más flexible y permite una mayor libertad en el establecimiento de estos derechos de propiedad.<sup>32</sup> Además, el derecho de propiedad en el derecho civil se considera un derecho *erga omnes*, es decir, tiene poder frente a terceros, mientras que el *common law* reconoce derechos personales de propiedad y derechos reales de propiedad (*in personam* y *in rem*).<sup>33</sup>

En el ámbito del IoT, la propiedad del objeto conectado -máquinas o aparatos- muchas veces no coincide con la titularidad de los datos que genera; por ello, llegar a dar una solución legal puede ser una difícil tarea, de ahí que sea uno de los principales debates y dilemas en la actualidad. Cabe señalar que muchos consideran el término **propiedad de los datos** (*data ownership*) incorrecto, prefiriéndose en su lugar el término *data control* (control de datos) que refleja en mejor medida los derechos que una persona u organización tiene sobre datos personales o no personales.<sup>34</sup>

Sobre esta misma idea, muchos opinan que los datos les pertenecen a los usuarios -sobre quién es el dato- mientras que, por otra parte, las empresas sostienen que los datos

---

<sup>31</sup> Comisión Europea, Staff Working Document, “On the free flow of data and emerging issues of the European data economy, accompanying COM (2017) 9 final”. SWD (2017), 2 final. EUR-LEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0002>

<sup>32</sup> Ver VAN ERP, AKKERMANS, B. *The principle of numerus clausus in European property law*, Intersentia, 2008; GORDLEY, J. *Foundations of Private Law: property, tort, contract, unjust enrichment*, OUP, 2006.

<sup>33</sup> *Ibidem*.

<sup>34</sup> VERMESAN O. FRIESS P. *Digitising the Industry. Internet of Things connecting the physical, digital and virtual worlds*. River Publishess (2016), p. 228

que recopilan y tratan son de su propiedad, ya que son los que han dedicado tiempo, dinero y otros recursos invertidos en diversos sistemas y tecnologías. La problemática no sólo concierne a los datos personales que son objeto de la normativa de protección de datos, sino también de otros datos producidos por una economía digital, donde gran parte de ellos son generados por máquinas o por sensores, aplicándose especialmente a los datos producidos en industrias («Industria 4.0») o desarrollados mediante IoT, que comprenden lo que a veces se denomina «*industrial data*» que no está protegido por los derechos exclusivos de propiedad.

Toda esta cuestión ha causado recientemente debates tanto en el seno de la UE como a nivel mundial, y ante la falta de legislación que regule el concepto y contexto del derecho de propiedad de los datos, se observa cada vez más la patente necesidad de un derecho que regule estos nuevos retos a los que la sociedad se enfrenta debido al aumento de las innovaciones tecnológicas en nuestro día a día.<sup>35</sup> Es por ello que la Comisión Europea está postulando el concepto de la propiedad de los datos como un derecho legítimo, pero la mayoría de la doctrina tiene ciertas reservas sobre el mismo.<sup>36</sup>

La Comisión Europea ha desarrollado esta cuestión en diversas Comunicaciones a lo largo de los últimos años, en la Comunicación de 2015<sup>37</sup> sobre “una estrategia para el Mercado Único Digital de Europa” ya se empezó a hablar sobre la necesidad de una regulación sobre la propiedad de los datos y el acceso. Posteriormente en la Comunicación de 2017<sup>38</sup> sobre “la construcción de una economía de los datos europea” se estableció que los datos en bruto generados por las máquinas no están protegidos por los derechos de propiedad intelectual (en adelante, PI). Y, más recientemente, la

---

<sup>35</sup> Tal y como dijo el comisario europeo Oettinger en su discurso de 2016 se necesita un guía legal para el IoT en la UE que trate sobre la protección de datos, la seguridad, reglas de responsabilidad y los problemas del derecho de propiedad y acceso a los datos: “*We need single rule book for the Internet of Things in Europe. Capable to properly address new challenges raised by the technology. This includes data protection, safety and liability rules, including the emerging issues of data ownership, rules on access and re-use of non-personal data in an industrial context, just to mention a few [...]*” Recuperado en: <https://ec.europa.eu/commission/2014-2019/oettinger/announcements/keynote-speech-closing-plenary-session-net-futures-2016-brussels.en>

<sup>36</sup> JANECEK, V. *Ownership of personal data in the Internet of Things*. Computer Law & Security Review (ELSEVIER Ltd.), vol. 34 nº.5, 2018. Recuperado de: <https://ora.ox.ac.uk/objects/uuid:7c49751d-83e2-4f8a-822e-1e669057eb10/>

<sup>37</sup> Comisión Europea, *A Digital Single Market Strategy for Europe* [Una Estrategia para el Mercado Único Digital de Europa], Comunicación, COM (2015) 192 final, 6 de mayo 2015. Recuperado en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192>

<sup>38</sup> *Op cit.* (Supra 7, pág. 9)

Comunicación de 2020<sup>39</sup> sobre “una estrategia europea de datos” ha anunciado la creación de normativa en ámbitos específicos, creando un espacio común europeo en datos sectoriales; en concreto, abordará en el cuarto trimestre de 2021 una normativa más amplia relacionada a cuestiones del derecho de uso sobre datos industriales (datos del internet de las cosas creados en los entornos digitales).<sup>40</sup>

*B) Las opciones tratadas en el ámbito de la propiedad*

En el ámbito del IoT se pueden identificar varios problemas a los que se debe hacer frente<sup>41</sup>, especialmente, en cuanto a los datos recopilados por los sensores -cuestión que abordamos en este trabajo-. A este respecto, como afirma Peppet<sup>42</sup>, estos datos son especialmente difíciles de identificar, y el consentimiento sobre el uso y la recopilación de información es un verdadero entramado de problemas dentro del ámbito del Internet de las Cosas.

A día de hoy, como resulta de lo expuesto en el epígrafe anterior, tampoco existe una regulación expresa en el derecho español sobre la propiedad de los datos generados por máquinas y dispositivos, requiriendo realizase un estudio y análisis legal sobre la propiedad caso por caso; ello, a pesar de las posibilidades de aplicar ciertas normativas, como, por ejemplo, la LSE que traspone la Directiva sobre Secretos Comerciales.

La escasa doctrina<sup>43</sup> que se ha ocupado de la propiedad de los datos se ha centrado en cuatro opciones para la resolución de este problema:

- (1) Desarrollar un derecho de propiedad de facto.

---

<sup>39</sup> Comisión Europea, *A European strategy for data* [Una estrategia europea de datos] Comunicación, COM (2020) 66 final, 19 de febrero 2020. Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0066>

<sup>40</sup> APPENDIX to the Communication ‘A European strategy for data’ «A 2018 study estimated the potential value of use of non-personal data in manufacturing at € 1,5 trillion by 2017 (Deloitte 2018). In order to unleash this potential, the Commission will: Address issues related to the usage rights on co-generated industrial data (Iot data created in industrial settings), as part of a wider Data Act (Q4 2021) [...]».

<sup>41</sup> Especialmente el profesor PEPPET mantiene que se pueden identificar cuatro problemas principales: (1) la discriminación, (2) la privacidad, (3) la seguridad y (4) el consentimiento. PEPPET, S. *Regulating the Internet of Things: First steps toward managing discrimination, privacy, security & consent*, 93 TEX. L. REV. 85 (2014).

<sup>42</sup> PEPPET S. *Regulating the Internet of Things: First steps toward managing discrimination, privacy, security & consent*, 93 TEX. L. REV. 85, 2014

<sup>43</sup> Cfr. Becker, M. (2017). Rights in Data–Industry 4.0 and the IP Rights of the Future. *Zeitschrift fuer Geistiges Eigentum/Intellectual Property Journal*, 9(3), 253-265; Berger, C. (2017). Property Rights to Personal Data? – An exploration of Commercial Data Law. En *Zeitschrift für Geistiges Eigentum – Intellectual Property Journal: 3 Band 9*, 340-355.

- (2) Aplicar la normativa de propiedad intelectual, relacionándolo con el derecho de *copyright*, es decir, los derechos de autor o con los derechos de las bases de datos.
- (3) Acogerse a la regulación de secretos comerciales/empresariales.
- (4) Confiar en una protección jurídica derivada de contratos firmados entre partes.

Las empresas *de facto* poseen los datos, vendiéndolos o permitiéndoles usarlos a terceros. Pero, no tienen la propiedad legal de los datos -en el sentido de propiedad exclusiva-, de ahí que haya surgido la controversia de la creación de un nuevo derecho de propiedad en el mercado digital de datos. Como ya se ha mencionado, nuestro Código Civil establece el concepto de «propiedad» en su artículo 348. Por lo tanto, entendemos que mientras no exista un contrato o acuerdo que regule la referida propiedad de los datos entre las partes implicadas, la única entidad o persona que debería tener derecho a disfrutar y disponer de los datos sería la que los ha generado/producido realmente. En este sentido, la información tendría un tratamiento similar a los frutos obtenidos de los bienes al pertenecer, si no hay otras circunstancias, al propietario del bien.

En cuanto al amparo dentro de la protección del derecho de propiedad intelectual, diversas normas internacionales y europeas -Acuerdo del GATT y OMC adoptado en Marrakech (1994) sobre aspectos de la propiedad intelectual relacionados con el comercio (Anexo 1C, art. 10), el Tratado de la OMPI sobre Derecho de Autor, Ginebra, el 20 de diciembre de 1996 (art. 5)<sup>44</sup> y la Directiva UE 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos<sup>45</sup> - han establecido que la propiedad intelectual sólo ampara los datos cuyos contenidos sean creaciones originales y señalan expresamente que esta protección no ampara a la información recopilada o a los datos en sí.

Los datos como bienes intangibles en realidad no pueden ser capturados como un ámbito protegido bajo el tradicional derecho de propiedad, aunque ciertas decisiones judiciales han equiparado la propiedad de los datos no personales a la bienes físicos que contienen esos datos.<sup>46</sup> Por ello, se procede a establecer las diferentes opciones que se

---

<sup>44</sup> WIPO Lex: TRT/WCT/001.

<sup>45</sup> DOUE: L 77 de 27 de marzo de 1996 modificada por L 130 de 17.5.2019 (Directiva (UE) 2019/790). EUR-Lex: <http://data.europa.eu/eli/dir/1996/9/2019-06-06>

<sup>46</sup> El Tribunal Supremo Federal Alemán (*Bundesgerichtshof*) el 15 de noviembre de 2006 sobre la propiedad de un software dentro de un CD-ROM. BGH 15.11.2006 (XII ZR 120/04) - Zur Rechtsnatur der

han planteado por diversos autores, siendo en primer lugar la posibilidad de protegerse mediante la Directiva 96/9/CE de 11 de marzo de 1996<sup>47</sup>, sobre la protección jurídica de las bases de datos, que protege a las bases de datos, en adelante Directiva de Bases de Datos, protegiéndose de esta manera los derechos de autor de la creación o por haberse realizado una gran inversión para crear dicha base de datos.

Esta Directiva de Bases de Datos protege a las bases de datos que constituyen una creación intelectual del autor o para las que sus fabricantes han realizado una denominada “inversión sustancial”. Aunque existen excepciones, el art. 7 de la Directiva protege a los autores o creadores de la base de un uso por terceros (por ejemplo, reproducción o reutilización y extracción del contenido), pero sólo en la medida en que sea la totalidad o partes sustanciales, o la utilización de partes insustanciales pero de manera “repetida y sistemática”.<sup>48</sup>

En particular, el derecho de autor sólo se aplicará si se alcanza un nivel mínimo de creatividad para poderse considerar como una “la creación intelectual propia del autor”, otorgando a dichas bases de datos el mismo nivel de protección del derecho de autor que a otras obras literarias. Pero en el caso de las bases de datos modernas es poco probable que la selección y disposición de los contenidos haya sido objeto de una habilidad y un juicio significativos, no existiendo tampoco una definición de “autor”.<sup>49</sup>

Parte de los datos del mercado digital están protegidos por la regulación del *copyright*, como son los e-books, softwares, música digital... Pero, en la actualidad, esta normativa no es la adecuada para aplicarse a gran parte de los activos digitales,

---

Softwareüberlassung im Rahmen eines ASP-Vertrages, Medien Internet und Recht, 01/2007: [http://medien-internet-und-recht.de/pdf/vt\\_MIR\\_Dok\\_009-2006.pdf](http://medien-internet-und-recht.de/pdf/vt_MIR_Dok_009-2006.pdf)

<sup>47</sup> DOUE: OJ L 77 de 27 de marzo de 1996 modificada por L 130 de 17.5.2019 (Directiva (UE) 2019/790). ELI: <http://data.europa.eu/eli/dir/1996/9/2019-06-06>

<sup>48</sup> Este derecho sólo protege a los inversores sustanciales en la base de datos, protegiéndola en su conjunto y no los datos específicos del contenido. El TJUE impidió una interpretación amplia del derecho de bases de datos que solo protegen una recopilación de hechos e información. Por tanto, los datos recogidos a través de sensores –esencialmente los datos digitales electrónicos-, quedan fuera de esta protección. Y, es bastante obvio que la Directiva de Bases de datos se basa en una tecnología de bases de datos que ya no corresponde al uso en una era del Internet de las Cosas, siendo demasiado estática para responder adecuadamente a la evolución de los servicios y productos en tiempo real.

<sup>49</sup> Además, la Directiva de Bases de Datos en su art. 3, dispone que «la protección de los derechos de autor de las bases de datos prevista por la presente Directiva no se extenderá a su contenido y se entenderá sin perjuicio de los derechos que subsistan sobre dichos contenidos». Esto fue confirmado por el TJUE en su decisión en el asunto C-604/10 Football DataCo c. Yahoo!6 del 1.03.12, donde sostuvo que una base de datos solo puede atraer los derechos de autor sobre su estructura y no su contenido, es decir, los datos propiamente dichos cuando estos no sean más que la recopilación de hechos preexistentes.

principalmente los creados por máquinas y recopilados por sensores, ya que no cumplen con los requisitos de la protección por *copyright*, no estando diseñado para los activos digitales como son los datos del IoT. Siendo que el derecho de autor (*copyright*) existe para proteger la autoría y la creatividad y no el conocimiento y la información «en bruto».

Adicionalmente, además del derecho de autor, las bases de datos gozan de protección jurídica a través del derecho *sui generis*, es decir, como un producto final comprendido en la protección de la normativa de propiedad intelectual. Sin embargo, aunque esto solucionaría la protección del dato una vez recabado e introducido en una base de datos, no soluciona al dato en sí, pues no son concebidos como un producto final.

Aun así, la protección ofrecida por esta normativa según la visión de la Comisión en la Comunicación de 2017<sup>50</sup>, no se aplica a los datos generados por máquinas como tal, en cuanto a los derechos de autor estos sólo cubren la autoría realizada por seres humanos, y el derecho *sui generis* exclusivamente cubre aquellos datos que están estructurados en las bases de datos, además de que en la mayoría de las empresas hay dificultad para demostrar una inversión sustantiva en sus bases de datos.<sup>51</sup>

Por tanto, las empresas sólo podrían tener la propiedad intelectual de la estructura de la base de datos (si es que es original, que no suele ser el caso) en sí. No por el hecho de poseer datos e información, procesarlo o almacenarlos se convierten en dueñas de dicha “información nominativa”, debido a que no existe en tal caso ningún título o modo de adquisición que son los elementos que se requieren para la propiedad. En conclusión, dado el acervo jurídico de la UE, éste apunta a una falta de seguridad jurídica sobre la titularidad de los datos no personales generados por las máquinas no estructurados en una base de datos protegida, ya que estos datos no pueden ser considerados fruto de un esfuerzo intelectual, así que este tipo de datos no pueden ser objeto de protección mediante los derechos de autor.

Sin embargo, también existen posiciones diferentes, como por ejemplo el del profesor Raúl Bertelsen, que dice que «se reconoce y protege el derecho de propiedad, sin que sea necesario para reconocer la existencia de una propiedad garantizada constitucionalmente que tenga un estatuto legal propio, pues basta para ello que de la vida

---

<sup>50</sup> *Op cit.* (supra 7, pág 9).

<sup>51</sup> MALGIERI, G. *Ownership of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?* Journal of Internet Law, 2016, vol. 20 no 5.



jurídica haya surgido una situación o una relación en que concurren las características propias del dominio»<sup>52</sup>

Por otra parte muy diferente, los datos comerciales y técnicos de cualquier tipo y, evidentemente las recopilaciones de datos (incluso en algunos casos los datos individuales), pueden ser protegidos por la regulación de la LSE, que fue traspuesta para cumplir con la normativa europea de la Directiva de Secretos Comerciales. Aunque, no todas las leyes de los Estados miembros tratan los secretos comerciales como una categoría abierta de cualquier información como un hecho confidencial.

En el caso de España, se exige que la empresa adopte una serie de medidas formales para poder identificar la información como secreto empresarial, aunque hay diferentes opiniones sobre si los datos industriales en bruto y los generados por máquinas y sensores pueden ser en absoluto tratados como un secreto empresarial, no estando claro cómo aplicar esta normativa a datos recogidos por sensores de las máquinas.

Además, dado el caso analizado se debe aclarar que la LSE permite expresamente la adquisición de secretos comerciales mediante ingeniería inversa<sup>53</sup>. Esto significa que los datos sobre la configuración de un producto no pueden ser protegidos como secretos comerciales desde aquel momento en el que dicho producto se comercializa en el mercado, aunque cuando estamos hablando de máquinas industriales que se venden en pequeñas cantidades directamente a usuarios finales cabe la posibilidad de protegerlo mediante la imposición de restricciones contractuales.

La LSE define al secreto empresarial de manera muy amplia siendo «cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero» (art. 1 LSE). Ofrece una protección específica para cada uno de los elementos considerados como datos comerciales tal y como explica el considerando 1 de la Directiva de Secretos Comerciales se protege a una gama amplia de conocimientos técnicos (*Know-how*) e información comercial, ya sea como un complemento o como una alternativa a los derechos de PI, consiguiendo proteger y permitir al creador obtener beneficios de su creación y realizar importantes innovaciones, desarrollo e

---

<sup>52</sup> BERTELSEN REPETTO, R. *Datos Personales: propiedad, libre iniciativa particular y respeto a la vida privada*, en Cuadernos de extensión jurídica N°5, Universidad de los Andes, 2001, pp. 120-121.

<sup>53</sup> La ingeniería inversa es la adquisición mediante el estudio, desmontaje o el ensayo de un producto u objeto que se haya puesto a disposición del público o en posesión legal del adquirente del objeto sin ningún tipo de restricción. (art. 2 LSE)

investigaciones. Por tanto, se puede considerar esta regulación mucho más apropiada para el procesamiento de datos en un mundo de algoritmos e IoT.

Consecuentemente, la normativa protege la adquisición, utilización y divulgación ilícitas de secretos comerciales, exigiendo una serie de requisitos (art 2.1. Directiva de Secretos Comerciales y art. 1 LSE):

- La materia debe ser secreta “en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas”
- Debe tener valor comercial debido a su secreto, ya sea potencial o real;
- Y, la persona que legalmente controla la información ha tomado medidas para mantenerla secreta.

Sin embargo, si la información protegida por la protección del secreto empresarial se adquiere legalmente de otra manera, incluso sin el permiso del titular del secreto empresarial, el titular del secreto empresarial no tiene ningún recurso contra la persona que posee la información. Esto muestra las características personales de la protección de los secretos comerciales, a diferencia de la protección general de los derechos de propiedad. Dicho esto desde una perspectiva mucho más teórica, no hay obstáculo legal para que los datos sean protegidos en virtud de la Directiva sobre Secretos Comerciales, y en consecuencia la Ley de Secretos Empresariales, aunque hay autores como Drexl<sup>54</sup> que piensan que esta algo anticuada, ya que los nuevos avances de la economía de datos no se tuvieron en cuenta durante el proceso legislativo de esta ley hace unos años.

Aun así, el cumplimiento de los requisitos de la Ley depende de los hechos, existiendo diversas cuestiones que deben de tenerse en cuenta. Por un lado, es previsible que los datos producidos internamente en una empresa sean calificados como secretos, pero los datos recogidos por sensores de uso público (como son los coches) puede que no satisfagan este requisito. Además, aunque es indudable que los datos tienen un alto valor comercial, es cuestionable si este valor proviene de ser secreto el mismo.

---

<sup>54</sup> DREXL, J. *Designing Competitive Markets for Industrial Data*. J. Intell. Prop. Info. Tech. & Elec. Com. L. 8, 2017.

Por último, hoy en día, el acceso a datos industriales de las máquinas se basa en acuerdos contractuales, resultado de negociaciones entre las partes, al ser libres de acordar lo que deseen respetando los límites de la libre voluntad de las partes -leyes, moral y orden público-, en relación con la propiedad, acceso, tratamiento o explotación de los datos. Además, las empresas, como CONER, que crean nuevos productos para mercados en una considerable rápida evolución requieren de una cierta flexibilidad para determinar una solución adecuada, y, por tanto, la solución contractual es una de las más adecuada, a pesar de poseer también ciertas desventajas, al requerir una exhaustiva negociación y alta especialización en la materia para poder negociar dicho tipo de acuerdos.

Hasta el momento, la UE sólo ha adoptado unas iniciativas limitadas en cuanto a derecho contractual, principalmente para la protección del consumidor, por tanto, no es probable que afecten a las transacciones B2B (entre empresas) y la capacidad de estas para acceder a los datos y controlarlos.

Sin embargo, en el plano nacional, la práctica más habitual entre las entidades es el derecho contractual, siendo todavía más importante su uso cuando los datos no son o no pueden considerarse secretos, y tampoco pueden ampararse en el derecho de propiedad intelectual. Por tanto, las cláusulas contractuales son utilizadas para aclarar los derechos de cada parte en relación con los datos y a la vez definir las restricciones aplicables, no existiendo ninguna razón por la cual no enmarcarse el derecho contractual en la gestión de los derechos sobre los datos.

Concluyendo este apartado cabe mencionar que los tribunales españoles no han tenido el suficiente tiempo como para pronunciarse sobre la propiedad de los datos, y la mayoría de la jurisprudencia presente hace referencia a los datos personales al ser la gran parte de las cuestiones planteadas a los tribunales relacionadas con los consumidores y no con otras empresas, siendo la autoridad encargada sobre las problemáticas la AEPD, añadiéndose además la continua evolución y novedad en el acervo legislativo y social sobre los datos generados por máquinas y del Big data.

En este sentido, un enfoque general aunque tácito sobre esta materia en España es, tal y como se afirma en la publicación de Situación Economía Digital de febrero de 2016 de BBVA<sup>55</sup>, los paradigmas actuales varían entre considerar como productor al productor

---

<sup>55</sup> Situación Economía Digital Febrero 2016, BBVA Research. Recuperado en: [https://bbvaresearch.com/wp-content/uploads/2016/02/Situacion\\_ED\\_feb16\\_Cap4.pdf](https://bbvaresearch.com/wp-content/uploads/2016/02/Situacion_ED_feb16_Cap4.pdf)

(el que genera los datos), el consumidor, el compilador (quien procesa los datos), la empresa (que controla la entrada y salida de datos), el sujeto de los datos, el comprador o licenciador, etc. En consecuencia, según la normativa de la UE el interesado es el propietario, es decir, el individuo que genera los datos de manera directa o indirecta - mediante desarrollo de un dispositivo para generar datos sin interacción de un tercero-, además que el interesado se define en el RGDP como “la persona física a la que pertenecen los datos objeto de tratamiento”, definición que se puede entender también traducible a aquellos datos que no sean personales. Sin embargo, se entiende en generar que la empresa que genera esos datos es el propietario incluso si ha requerido de un dispositivo o sensor de tercero.

## 5. CONCLUSIONES SOBRE EL DICTAMEN

### 5.1. Soluciones basadas en la titularidad de los datos de CONER

Tal y como se ha expuesto a lo largo de este trabajo, hasta la fecha no existe ninguna disposición legal o jurisprudencia expresa que se refiera a la cuestión de propiedad de los datos en España. Por lo tanto, se debería realizar un análisis *ad hoc* tanto sobre los principios legales generalmente aceptados que afectan a los datos, como sobre el concepto de propiedad en España, si no existe un contrato entre las partes implicadas para regular la propiedad de los datos. Pudiéndose decir que el concepto de titularidad de los datos se interpreta a partir del concepto de titularidad, y por tanto el titular tendría derecho a disfrutar y disponer de los datos.

Pero, en la práctica, lo más usual es que las empresas realicen acuerdos sobre la propiedad de los datos, acceso y tratamiento de los mismos. De este modo, en tanto que las partes son prácticamente libres para acordar en mejores términos, siempre que se observen los límites de la voluntad de las partes, podrán acordar también las consecuencias del incumplimiento de cualquiera de las previsiones de mutuo acuerdo establecidas en un contrato. Es por todo ello, la importancia de los acuerdos contractuales que pueden basarse en diferentes modelos; siguiendo una propiedad única o una propiedad conjunta de los datos recopilados. En cualquier caso, los acuerdos deben tratar también otras materias importantes en el ámbito del IoT, como por ejemplo el espionaje industrial, la competencia desleal, etc.

Consecuentemente, una de las mejores soluciones para CONER sería establecer unas cláusulas contractuales, al no existir entre la información recogida datos sensibles o

personales -basándonos en la voluntad de las partes-, expresadas en los contratos con los compradores y arrendadores de sus máquinas, con el fin de asegurarse de que el tratamiento de los datos que realiza no pueda ser posteriormente demandado por estos. Es por ello que una de las posibles cláusulas a incorporar en los contratos puede ser la siguiente:

*«CONER será el propietario único y exclusivo de todos los datos generados por los dispositivos, entre otros y sin limitación, todos los conocimientos técnicos, algoritmos matemáticos, procedimientos, métodos y operaciones, que no se correspondan con datos personas de personas identificadas o identificables, así como todos los derechos de propiedad intelectual e industrial que se pudieran derivar de su explotación. CONER no asume ninguna responsabilidad ni será titular de ningún dato personal de los clientes y trabajadores, cuya titularidad y responsabilidad se atribuye exclusivamente a YYY (Comprador)»*

Pero, el problema no sólo se encuentra en la titularidad o propiedad de dichos datos, sino que se debe reforzar dichas cláusulas con otras que aseguren la recolección de los datos y la no cesión de los datos por los clientes de CONER. Con ello, aparte de centrarse en establecer cláusulas de atribución de propiedad de los datos al fabricante -CONER-, se deben crear cláusulas de omisión y prohibición de cualquier conducta que pueda obstaculizar la recolección de los datos y llegada a la nube, además de la prohibición del uso/acceso a los datos por el propio cliente. Incluso es compatible con el establecimiento de un acuerdo de confidencialidad y no divulgación (NDA) firmado por las partes.

Una de las posibles cláusulas, acumulada a la anterior de propiedad, puede ser la siguiente:

*«El cliente no podrá obstaculizar en ningún caso la recopilación de los datos mediante los sensores y otros dispositivos incorporados al producto, ya sea mediante la alteración de los propios dispositivos, del producto o de la conexión y transmisión de estos. El cliente se obliga a no acceder o usar los datos recopilados por ningún medio y, si de alguna manera estos llegaran a su conocimiento deberá informar de inmediato a CONER manteniéndose en todo caso la información confidencial».*

## 5.2.Soluciones basadas en la protección de los datos de CONER como secreto empresarial

Adicionalmente, es conveniente que todos los acuerdos que se tomen en la empresa para poder garantizar la utilización de los datos generador por el objeto del IoT -la maquinaria- puedan regularse teniendo en cuenta la Ley 1/2019 de 20 de febrero, de Secretos Empresariales, en adelante LSE, normativa transpuesta por la Directiva de Secretos Comerciales, reforzando de tal manera la propiedad del fabricante de la maquina.

Un secreto empresarial puede ser definido como cualquier información o conocimiento de carácter tecnológico, comercial, científico, industrial, financiero u organizativo que cumpla con una serie de requisitos que se han mencionado anteriormente. Además, el Código Penal español, en sus artículos 278 y 279 condena a quienes revelen a terceros los secretos que se han accedido como consecuencia de relación laboral o secretos de los cuales el infractor haya contraído una obligación de confidencialidad. Es por el ello que el TS<sup>56</sup> ha expuesto los criterios que deben aplicarse para determinar la existencia de un “secreto empresarial” para poder interpretar las deposiciones del CP, definiendo al secreto empresarial de una manera amplia como «toda información, que en caso de ser revelada, afecte a la competitividad de la empresa en el mercado», considerando que tanto los secretos comerciales, meramente organizativos como los técnico-industriales, pueden comprenderse en esta definición si son propiedad exclusiva de la empresa, son confidenciales y económicamente valiosos para sus actividades empresariales.

### 1. El dato es **secreto**, no es conocido o accesible fácilmente. (art 1.1.a LSE).

El secreto, es uno de los principales requisitos, es decir, no tiene que ser en su conjunto conocida, ni fácilmente accesible, para ello se debe identificar de forma correcta qué información y datos son susceptibles de ser secretos, al existir diversos tipos de datos.<sup>57</sup> En el caso de los datos creados por una máquina, los datos industriales pueden

---

<sup>56</sup> Sentencia Tribunal Supremo, Sala Segunda de lo Penal, de 12 de mayo de 2008, nº resolución 285/2008. ECLI: ES:TS:2008:2885 Recuperado en CENDOJ: <http://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703>

<sup>57</sup> Los datos pueden ser de diferentes tipos, datos personales, datos que no están protegidos ni por derechos de propiedad intelectual como lo son los producidos por sensores de maquinaria, tal y como considera Kerber, datos no personales, datos anonimizados, datos generados por máquinas que pueden ser personales o no personales, etc. Además también se pueden diferenciar según Kerber en función de donde provengan (capturados pro sensores, derivados de otras fuentes, datos voluntariamente por el usuario), o incluso según el profesor Zech en función del contenido de los datos, semántico o sintáctico.

cumplir con los requisitos de secretismo, en los términos de la LSE, ya sea como una combinación de datos o un conjunto de datos. En efecto, la Comisión considera que los datos generados individualmente no pueden poseer un valor comercial, cosa diferente para el caso del conjunto de datos.<sup>58</sup>

2. Tiene un valor comercial. (art. 1.1.b. LSE).

A continuación debemos poder constatar como ese conjunto o combinación de datos son un activo que es muy capaz de determinar el éxito del negocio<sup>59</sup>. En este sentido, existen autores que consideran que se puede proteger como secreto empresarial el software, los documentos técnicos, la metodología e incluso el código fuente de los software.<sup>60</sup> Consecuentemente, los datos que la empresa está recabando son un importante activo de la empresa que les permite mejorar y continuar innovando en los productos que fabrica, poseyendo por tanto un valor empresarial –aunque indirecto- a través de la necesidad que tienen para poder obtener una ventaja competitiva y posicionarse en el mercado con unos productos mejorados debido al análisis secreto de estos datos recabados.

3. Ha sido sometido a ciertas circunstancias para poder mantenerlo en secreto. (art. 1.1.c. LSE).

Es tercer lugar, va a ser necesario realizar un mantenimiento diligente y razonable del secreto, dado que el umbral de protección del secreto empresarial requiere que se mantenga en secreto en todos los sentidos, semántico y sintáctico.

Es por ello que, para que todos los datos que la empresa recoja a través de los sensores de la maquinaria posean carácter secreto, no ha de permitirse que un tercero acceda a los mismos. Al establecer un canal que recoge los datos y directamente los trasmite a las bases que la empresa posee en sus oficinas, se puede concluir que dicha información está en todo momento mantenida en posesión de la empresa, y, por tanto,

---

<sup>58</sup> Op. Cit. (Supra 6, pág.9).

<sup>59</sup> Tal y como decía Marr: «(...) la capacidad de una empresa para competir será cada vez más impulsada por lo bien que puede aprovechar los datos, aplicar los análisis e implementar nuevas tecnologías. (...) En los negocios, la información es poder, y el Big data está proporcionando información que no habríamos soñado con recoger o analizar hace años. Las empresas que no evolucionan y abrazan la revolución de los datos se quedarán atrás». MARR, B., *Data Strategy*, Great Britain, Kogan Page Limited, 2017.

<sup>60</sup> Expresiones concluidas de la Webinar realizada por Simón Valverde, socio de Arias Law y Andy Ramos, Counsel de Propiedad Industrial Intelectual y Tecnología de Pérez-Llorca. <https://elderecho.com/la-proteccion-juridica-del-software-secreto-empresarial>

secreta – salvo las correspondientes medidas que se deben de aplicar y analizar si estamos ante un servicio de *cloud computing* prestado por terceros a la empresa, no siendo este análisis objeto de este trabajo-.

Por ello, CONER se debe de encargar de adoptar las medidas razonables para proteger estos datos del conocimiento externo, realizando las inversiones necesarias, por ejemplo en lo referente a medidas de ciberseguridad y evitar ataques a sus servidores o incluso medidas contra el espionaje industrial. Para ello, es recomendable establecer alguna solución tecnológica que refuerce el flujo de los datos, pasando desde la máquina directamente a la central de la empresa, sin que se pueda acceder a estos datos por parte de ningún tercero ajeno a CONER, siendo una de las posibles opciones la encriptación de los mismos. Pero, además, de adoptar una serie de medidas razonables dirigidas a los datos para su protección y mantenimiento del secreto, ello debe combinarse con medidas dirigidas a los sujetos que real o potencialmente puede tener acceso a los mismos, por lo que será preciso celebrar acuerdos o establecer cláusulas de confidencialidad.

Si se consigue establecer este conjunto de medidas de seguridad se podrá entender que los datos recabados pueden ser protegidos a través del secreto empresarial, aparte de la protección concedida por las diferentes cláusulas contractuales establecidas en los diferentes contratos con los clientes.



### III. CONCLUSIONES FINALES

Se ha podido observar como en los últimos años el problema expuesto en este trabajo ha estado en la superficie de la discusión europea, estableciéndose en la más reciente Comunicación de la Comisión (2020) sobre “Una estrategia europea de los datos” la patente necesidad de una regulación marco que permita a las entidades reunir y utilizar los datos con el fin de mejorar los productos y permitir competir a nivel internacional de una manera mucho más eficaz. De ahí que esté presente en la estrategia de 2019-2024 la implementación de una estrategia industrial y de creación de un mercado de datos industriales. Incluso la UE necesita garantizar unas eficientes políticas de propiedad intelectual que pueda atender a los nuevos retos que la sociedad se enfrenta, y de esta manera ayudar a todas las empresas a crecer y desarrollarse obteniendo una ventaja competitiva.

Las dos opciones de la Comisión para incluir los derechos sobre los datos industriales o los denominados datos generados por máquinas, que son no personales o anonimizados son: la creación de un derecho real o la creación de un derecho puramente defensivo, como lo es la legislación del secreto empresarial, aunque también cabe establecer ciertas excepciones a esta propiedad de los datos como por ejemplo para un interés del sector público o para las investigaciones científicas.<sup>61</sup>

Por consiguiente, ante la falta de regulación e incertidumbre sobre la «propiedad» de los datos, las empresas se deben centrar en dos opciones compatibles; el derecho contractual y el secreto empresarial, ya que no se pueden encontrar dentro de la protección de derechos de autor o propiedad intelectual los datos en bruto sólo confiriéndose dicha protección a los datos estructurados y organizados en una base de datos.

A lo largo del trabajo se han observado diversos argumentos a favor de reconocer un grado de propiedad o titularidad a los productores de datos, porque necesitan libertad para llevar a cabo sus negocios y para proteger sus inversiones ya que los datos otorgan una ventaja competitiva. Sin embargo, es innegable que los diferentes tipos de datos desempeñan un importante papel ya que, la protección depende de ello siendo diferente si los datos se han generado con aportes del usuario o si fue debido a una actividad principal de la empresa. Aquí los secretos comerciales adquieren especial relevancia, pero

---

<sup>61</sup> COMISION EUROPEA, Staff Working Document accompanying the Communication from the European Commission “Building a European data economy”, (Brussels, 10.01.2017), SWD(2017) 2 final p. 33 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN>

hay que hacer hincapié que no hay un derecho exclusivo de propiedad, sino que es un mero derecho defensivo lo que regula esta legislación para proteger los datos.

Aun así, la solución más idónea que por el momento existe ante esta problemática es la solución contractual, siendo una de las opciones que todas las empresas más apuestan. Además, al estar ante un mundo globalizado y debida a la existencia de diversas legislaciones es todavía más conveniente la regulación contractual en vez de atender a un imperativo legal que puede cambiar en cada supuesto concreto.

En relación a esto último, he de decir que, al ser un intercambio de datos no personales o no anónimos, lo contrario que sucedería si fuesen personales al tener que garantizarse una mayor seguridad y protección para protegerse los derechos de las personas, podrían reducirse ciertas problemáticas si existiesen unas “disposiciones modelo” para las cláusulas contractuales o para las licencias de uso de datos. De esta manera, al obtener un conjunto de condiciones contractuales recomendadas por ciertas autoridades en colaboración con, por ejemplo, asociaciones industriales y expertos en la materia, podría crear un mayor equilibrio para las pequeñas empresas y ofrecer una mayor seguridad jurídica sin dejar, claro está, de salvaguardar y permitir la libertad contractual entre las partes.

En conclusión, la mejor solución ante datos no personales recopilados en el ámbito del IoT será una combinación de cláusulas contractuales que aseguren la propiedad, o mejor dicho titularidad, de los datos recopilados junto con cláusulas que aseguren que los clientes personas jurídicas no puedan obstaculizar la recopilación y envío, acceder o hacer uso de estos datos. Además, de un fortalecimiento de la protección gracias a las medidas que confiere la LSE al declarar estos datos un secreto empresarial, debido a su importante valor comercial y empresarial al poder ofrecer una ventaja competitiva en el mercado, siendo necesario establecer ciertas medidas tecnológicas para su mantenimiento como secreto frente a terceros.

#### IV. BIBLIOGRAFÍA

##### a) Fuentes doctrinales

BECKER, M. *Rights in Data–Industry 4.0 and the IP Rights of the Future*. Zeitschrift fuer Geistiges Eigentum/Intellectual Property Journal, 9(3), 2017, pp. 253-265

BERTELSEN REPETTO, R. *Datos Personales: propiedad, libre iniciativa particular y respeto a la vida privada*, en Cuadernos de extensión jurídica N°5, Universidad de los Andes, 2001, pp. 120-121.

BERGER, C. *Property Rights to Personal Data? – An exploration of Commercial Data Law*. En *Zeitschrift für Geistiges Eigentum – Intellectual Property Journal: 3 Band 9*, 2017, pp. 340-355.

CASTAÑOS CASTRO, P.; CASTILLO PARRILLA, J. A. «Capítulo 8: Economía digital y datos entendidos como bienes», en *El Mercado digital en la Unión Europea*, Pastor García, A.M. y Martens Jiménez, I.L. (coord.), 1ª ed., Reus Editorial, Madrid, 2019.

DIÉZ-PICAZO, L. *Fundamentos del derecho civil patrimonial. Las relaciones jurídico-reales. El registro de la propiedad. La posesión*. Civitas, t. III, 5ª ed., Madrid, 1996, p.159.]

D'SOUZA, C. *Big data and Trade Secrets (A general Analysis)*. Research Paper, Master of Law in Intellectual Property (Turin), 15 Enero 2019, Recuperado en <https://ssrn.com/abstract=3316328> o <http://dx.doi.org/10.2139/ssrn.3316328>

DREXL, J. et al, *Data Ownership and access to Data-position statement of the Max Planck Institute for Innovation and Competition Research paper*. Max Planck Institute for Innovation & Competition Research Paper, a 16 de Agosto de 2016.

DREXL, J. *Designing Competitive Markets for Industrial Data*. J. Intell. Prop. Info. Tech. & Elec. Com. L. 8, 2017.

GÓMEZ SEGADE, J.A., *Los bienes inmateriales en el Anteproyecto de Ley del Código Mercantil*. En: Estudios sobre el futuro Código Mercantil, Universidad Carlos III, 2015, pp. 115-135.

GRUPO DE TRABAJO DEL ARTÍCULO 29 “Opinion 4/2007 on the Concept of Personal Data”. (2007). WP 136 del 20 de junio de 2006.

GRUPO DE TRABAJO del art. 29, *Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos* adoptado el 16 de septiembre de 2014. 1471/14/ES WP. 223  
Recuperado en: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223\\_es.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf)

GORDLEY, J. *Foundations of Private Law: property, tort, contract, unjust enrichment*, OUP, 2006.

HARTZOG, W.; SELINGER, E. *The Internet of heirlooms and disposable things*. NCJL & Tech., Vol 17, 2016.

HEVERLY, R.A. (2003), *The information semicommons*, Berkeley Technology Law Journal, 18(4), pp. 1128-1189.

JANECEK, V. *Ownership of personal data in the Internet of Things*. Computer Law & Security Review (ELSEVIER Ltd.), vol. 34 n°5, 2018. Recuperado de: <https://ora.ox.ac.uk/objects/uuid:7c49751d-83e2-4f8a-822e-1e669057eb10/>

KERBER, W. *A new (Intellectual) Property Right for non-personal data? An Economic analysis*, Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int), 2016. Recuperado en: <https://ssrn.com/abstract=2858171>

MALGIERI, G. *Ownership of Customer (Big) Data in the European Union: Quasi-property as comparative solution?*, Journal of Internet Law, vol. 20, n° 5, 2016.

MARR, B., *Data Strategy*, Great Britain, Kogan Page Limited, 2017.

MATA AGÜERO, M. *Industrial data and trade secrets: A balanced approach or an excessive mismatch?* Tesis Universidad Técnica de Munich, Alemania, 2018. Dir. Ansgar Ohly. <http://repositorio.conicit.go.cr:8080/xmlui/handle/123456789/262?show=full>

MUELLER-LANGER, F.; MARTENS B.; DUCH-BROWN, N., *The economics of ownership, access and trade in digital data*, Digital Economy Working Paper 2016-10, JRC Technical Reports.

OSBORNE CLARKE, LLP. *Legal study on Ownership and access to Data*. European Commission, 2016. DOI:10.2759/299944 <https://op.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1>

PEPPET, S. *Regulating the Internet of Things: First steps toward managing discrimination, privacy, security & consent*, 93 TEX. L. REV. 85, 2014

PURTOVA, N. *The law of everything: Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology 10(1), pp. 40-81, 2018 DOI: [10.1080/17579961.2018.1452176](https://doi.org/10.1080/17579961.2018.1452176)

REMOLINA ANGARITA, N.; TAFUR NADER, G. “Limitaciones de las cláusulas contractuales para determinar la naturaleza jurídica de la información y para proteger los secretos empresariales” Revista La Propiedad Inmaterial nº 24, Universidad Externado de Colombia, julio-diciembre 2017, pp. 145-165. DOI: <https://doi.org/10.18601/16571959.n24.07>

STEPANOV, I. *Introducing a property right over data in the UE: the data producer’s right – an evaluation*. International Review of Law, Computers & Technology, 34:1, 2020, pp. 66-86 DOI: <https://doi.org/10.1080/13600869.2019.1631621>

THOUVENIN, F. et al. *Data ownership: Taking stock and mapping the issues*. En Frontiers in Data Science. CRC Press, 2017.

TORRE DE SILVA, J. *El Derecho Civil de los datos*, Anuario de Derecho Civil: Tomo LXXII, fasc. III pp. 825-877, 2019.

VAN ERP, AKKERMANS, B. *The principle of numerus clausus in European property law*, Intersentia, 2008.

VERMESAN O. FRIESS P. *Digitising the Industry. Internet of Things connecting the physical, digital and virtual worlds*. River Publishess pp. 228, 2016.

WORLD ECONOMIC FORUM, *Personal data: the emergence of a new asset class* (2011). Disponible en: <https://www.weforum.org/reports/personal-data-emergence-new-asset-class>

ZECH, H. *Building a European Data Economy – The European Commission’s Proposal for a Data Producer’s Right*, Intellectual Property Journal vol. 9, pp. 317-330, 2017.

ZECH, H. *Information as Property*, JIPITEC 192 6, 2015.

#### **b) Documentos legislativos y propuestas**

Comisión Europea. “Comisión Europea. *Building a European Data Economy*. [La Construcción de una Economía de los Datos Europea], Comunicación, COM (2017) 9 final, 10 de enero 2017. Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017DC0009>

Staff Working Document accompanying the Communication from the European Commission “Building a European data economy”, (Brussels, 10.01.2017), SWD(2017) 2 final p. 33 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN>

Comisión Europea, Staff Working Document, “*On the free flow of data and emerging issues of the European data economy, accompanying COM (2017) 9 final*”. SWD (2017), 2 final. EUR-LEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0002>

Comisión Europea, *A Digital Single Market Strategy for Europe* [Una Estrategia para el Mercado Único Digital de Europa], Comunicación, COM (2015) 192 final, 6 de mayo 2015. Recuperado en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192>

Comisión Europea, *A European strategy for data* [Una estrategia europea de datos] Comunicación, COM (2020) 66 final, 19 de febrero 2020. Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0066>

### c) Fuentes jurisprudenciales

Sentencia del TJUE (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland Ltd*, asuntos acumulados C-293/12 y C-594/12, EU:C:2014:238 apartado 52, Recuperado en: <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62012CJ0293>

Sentencia del TJUE (Sala Tercera) de 7 de noviembre de 2013, *IPI vs Englebert*, C-473/12, EU:C:2013:715, apartado 39, Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0473>

Tribunal Supremo Federal Alemán (Bundesgerichtshof) el 15 de noviembre de 2006 sobre la propiedad de un software dentro de un CD-ROM. BGH 15.11.2006 (XII ZR 120/04) - Zur Rechtsnatur der Softwareüberlassung im Rahmen eines ASP-Vertrages, Medien Internet und Recht, 01/2007: [http://medien-internet-und-recht.de/pdf/vt\\_MIR\\_Dok\\_009-2006.pdf](http://medien-internet-und-recht.de/pdf/vt_MIR_Dok_009-2006.pdf)

Sentencia del TJUE asunto C-604/10, de 1 de marzo de 2012, *Football DataCo c. Yahoo!*6. Recuperado en Curia: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=609669D3BEDFC4BF0>

[B70CFDA92EAFB76?text=&docid=119904&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=5453666](http://www.poderjudicial.es/tribunales/tribunal-supremo/contenidos/ver_documento?text=&docid=119904&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=5453666)

Sentencia Tribunal Supremo, Sala Segunda de lo Penal, de 12 de mayo de 2008, nº resolución 285/2008. ECLI: ES:TS:2008:2885 Recuperado en CENDOJ: <http://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703>

#### **d) Consultas artículos y páginas de Internet**

BAZARRA, I. “Los datos, la materia prima del siglo XXI”, Tendencias KPMG, 2019 [consultado el 14 junio 2020] Disponible en: <https://www.tendencias.kpmg.es/claves-decada-2020-2030/datos-privacidad-monetizacion/>

“La protección jurídica del software como secreto empresarial” en Elderecho.com, de 27 del abril de 2020 <https://elderecho.com/la-proteccion-juridica-del-software-secreto-empresarial>

Regulación de los datos generados por máquinas: “menos es más” en aras del crecimiento mundial. OMPI REVISTA, diciembre de 2017. [https://www.wipo.int/wipo\\_magazine/es/2017/06/article\\_0005.html](https://www.wipo.int/wipo_magazine/es/2017/06/article_0005.html)

Situación Economía Digital Febrero 2016, BBVA Research. Recuperado en: [https://bbvaresearch.com/wp-content/uploads/2016/02/Situacion\\_ED\\_feb16\\_Cap4.pdf](https://bbvaresearch.com/wp-content/uploads/2016/02/Situacion_ED_feb16_Cap4.pdf)