Universidad Zaragoza
1542

Trabajo Fin de Grado

Mecanismos jurídicos para la protección de soluciones de *machine learning*.

Autora

Paula Ruiz Lozano

Director

Pedro-José Bueso Guillén

Elaborado en colaboración con ITAINNOVA

FACULTAD DE DERECHO

AÑO 2019

ÍNDICE

ABREVIATURAS

ADPIC	Acuerdo de Derechos de Propiedad Intelectual relacionados con el Comercio
DBD	Directiva sobre la protección jurídica de bases de datos.
DMUD	Directiva sobre los derechos de autor en el mercado único digital
DSE	Directiva de Secretos Empresariales
LCD	Ley de Competencia Desleal
LSE	Ley de Secretos Empresariales
TJUE	Tribunal de Justicia de la Unión Europea
TRLPI	Texto refundido de la Ley de Propiedad Intelectual
UE	Unión Europea

I. PRESENTACIÓN

1. ENFOQUE Y OBJETIVOS

El objeto del presente trabajo es el análisis de las diferentes opciones legales que permiten a los creadores de *machine learning* proteger su uso frente a terceros.

Tal y cómo se estudiará más detalladamente, el *machine learning* es una disciplina científica en el ámbito de la inteligencia artificial que crea sistemas que "aprenden" automáticamente. El término "aprender" se refiere a que el sistema es capaz de identificar patrones entre millones de datos gracias a algoritmos. De forma simplificada, los componentes del *machine learning* son, de una parte, los algoritmos, esto es, secuencias de instrucciones que representan un modelo de solución para un determinado tipo de problema y, de otra parte, el *big data*, esto es, grandes bases de datos que por su magnitud dificultan su gestión humana[1].

A grandes rasgos, el objeto de trabajo es analizar la protección jurídica del *big data* y los algoritmos. Al ser un campo muy novedoso, la legislación y la jurisprudencia en esta materia se renuevan constantemente.

En relación con los algoritmos, será preciso analizar la Ley 1/2019, de 20 de febrero, de Secretos Empresariales[2] (en adelante, LSE), en particular la violación de los secretos empresariales y las acciones de defensa de los mismos. Por supuesto, esto conllevará hacer referencia a la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de 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[3] (en adelante, DSE). El objetivo de la iniciativa europea es, por un lado, garantizar que la competitividad de las empresas y organismos de investigación europeos que se basa en el saber hacer y en información empresarial no divulgada (secretos empresariales) esté protegida de manera adecuada y, por otro,

---

[1] ANDRÉS GONZÁLEZ "¿Qué es Machine Learning?", 2014, Artículo de *Clever Data Big Data Prediction*. Disponible en: https://cleverdata.io/que-es-machine-learning-big-data/ [Consulta 26/03/2019]

[2] Publicado en: «BOE» núm 45, de 21-2-2019. Referencia: BOE-A-2019-2364

[3] Publicado en: «DOUE» núm. 157, de 15 de junio de 2016, páginas 1 a 18 (18 págs.). Referencia: DOUE-L-2016-81073

mejorar las condiciones y el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos en el mercado interior (cdo. 2.º DSE).

La protección legal del *big data* difiere de la anterior debido a que, en este caso, es aplicable el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (en adelante TRLPI)[4]. Así, en dicha norma se regulan dos formas de protección que nos interesan en el presente trabajo; por un lado, los derechos de autor que protegen la estructura de las bases de datos y, por otro lado, el derecho "sui generis" que protege la inversión sustancial del promotor en la base de datos. Se hará hincapié en la problemática aplicación del TRLPI cómo mecanismo de protección del *big data* debido a que el concepto de base de datos recogido en la Ley no se identifica con el concepto de *big data.*

Durante el trabajo, se hará referencia a diversa jurisprudencia relevante respecto del objeto del presente trabajo, cuyo análisis se irá desarrollando a lo largo de éste. No obstante, señalar que, debido a la reciente incorporación de la LSE, en cuanto a la protección del algoritmo, predominará la referencia a jurisprudencia nacional relativa a la Ley 3/1991, de 10 de enero, de Competencia Desleal (en adelante, LCD)[5]. Por último, en cuanto a la protección del *big data,* predominará jurisprudencia europea.

En definitiva, el objeto fundamental del presente Trabajo de Fin de Grado es responder a la siguiente pregunta "¿Qué mecanismos jurídicos de protección están a disposición de los creadores de *machine learning*?".

2. JUSTIFICACIÓN DEL INTERÉS

El desarrollo creciente de las nuevas tecnologías, del uso de internet y de las redes sociales han generado una gran cantidad de datos que mediante el *machine learning* nos proporcionan información muy valiosa aplicable a diferentes campos como la medicina, búsqueda online, reconocimiento facial, procesamiento del lenguaje natural, entre otros.

Al margen del interés objetivo de la problemática que se aborda en este trabajo, debe de ponerse de relieve que el mismo se realiza en colaboración con ITAINNOVA, quien

[4] Publicado en: «BOE» núm. 97, de 22 de abril de 1996, páginas 14369 a 14396. Referencia: BOE-A-1996-8930

[5] Publicado en: «BOE» núm. 10, de 11 de enero de 1991, páginas 959 a 962. Referencia: BOE-A-1991-628

contactó con el Grupo de Investigación de Referencia de Aragón sobre sobre "Gestión jurídica de negocios, instrumentos y organizaciones innovadoras" (LegMiBIO), del que el director de este trabajo es investigador principal, y manifestó su interés por dicha problemática y la elaboración de un Trabajo Fin de Grado sobre la misma.

En efecto, una de las entidades que más está apostando por el desarrollo del *machine learning* a nivel regional es el Instituto Tecnológico de Aragón (en adelante, ITAINNOVA). Dicha entidad es un instituto tecnológico, con personalidad jurídica propia, sin ánimo de lucro y cuyos fines son de interés general, que fue legalmente constituido a iniciativa del Gobierno de Aragón en el año 1984. La misión de ITAINNOVA es ayudar a las empresas aragonesas y promover las posibilidades tecnológicas de esta región, para desarrollar nuevos productos y procesos, con el propósito de impulsar la competitividad empresarial en Aragón, España y la UE[6].

ITAINNOVA, invirtiendo grandes cantidades de recursos y tiempo, ha desarrollado su producto "Moriarty", una herramienta de diseño e implementación de soluciones avanzadas de *software* de inteligencia artificial que permite resolver diferentes problemáticas de negocio mediante el análisis de grandes volúmenes de datos (*big data*). Concretamente, permite entender y estructurar la información e identificar patrones y correlaciones ocultas en los datos y, de esta forma, obtener predicciones útiles para las empresas usuarias[7].

Desde su creación, la herramienta Moriarty ha ido evolucionado de forma que, actualmente, se ofrecen las siguientes variantes del producto original en función de las necesidades de las empresas usuarias: "Social Moriarty", producto especializado en el análisis inteligente de medios sociales; "Search Moriarty", producto especializado en la búsqueda semántica inteligente; "Suggesting Moriarty", producto especializado en proporcionar recomendaciones inteligentes; "Profiling Moriarty", producto especializado en el perfilado inteligente de usuarios; "Insights Moriarty", producto

[6] Instituto Tecnológico de Aragón, 2018, Disponible en: https://itainnova.es/es/itainnova [Consulta 26/03/2019]

[7] Instituto Tecnológico de Aragón, Moriarty Web: Prototipado de soluciones inteligentes en Big Data, 2018. Disponible en: http://www.ita.es/moriarty/?showcase_moriarty_profiling.json [Consulta 27/03/2019]

especializado en la extracción inteligente de nuevos conceptos, y "Analytics Moriarty", producto especializado en el análisis inteligente de *big data*[8].

El gran valor que Moriarty ofrece es que posibilita la conversión de datos en valiosa información, de manera ágil, precisa y sencilla, facilitando la toma de decisiones estratégicas. Además, su capacidad para utilizar técnicas avanzadas de análisis semántico le otorga un valor diferencial que hace de Moriarty una herramienta única[9].

Sin embargo, el desarrollo de este proyecto de *machine learning* viene asociado a determinados riesgos a los que hacer frente. En primer lugar, el desarrollo tecnológico hace que sea cada vez más fácil la sustracción de la información, debido a que, al ser digital siempre puede ser *hackeada* por personas ajenas a ITAINNOVA, por ejemplo, por competidores. En segundo lugar, miembros de la propia entidad pueden acceder a ella, descargarla y publicarla o comercializar con ella.

La obtención, utilización o revelación ilícitas de la información sustraída comprometen la capacidad del ITAINNOVA para aprovechar las ventajas que le corresponden como precursor por su labor de innovación. La tardía regulación de instrumentos jurídicos eficaces y comparables para la protección de los distintos elementos del *machine learning* menoscaba los incentivos para emprender actividades asociadas a la innovación e impiden que este campo de la inteligencia artificial pueda liberar su potencial como estímulo del crecimiento económico y del empleo. En consecuencia, la innovación y la creatividad se ven desincentivadas y disminuye la inversión, con las consiguientes repercusiones en el buen funcionamiento del mercado y la consiguiente merma de su potencial como factor de crecimiento (véase cdo. 4.º DSE).

Por las razones anteriormente expuestas, es necesario un cuerpo legal que proteja adecuadamente este tipo de proyectos y que, a su vez, se adapte a los nuevos cambios tecnológicos producidos en el ámbito de la inteligencia artificial. Centrándonos en España, la protección de la inteligencia artificial se encuentra disgregada debido a que el *big data* se encuentra protegido por el TRLPI mientras que los algoritmos son protegidos por la LSE. La inexistencia de regulación jurídica específica que proteja un proyecto de *machine learning* en su conjunto genera una gran inseguridad para sus creadores.

---

[8] Instituto Tecnológico de Aragón, Moriarty Web: Prototipado de soluciones …*op. cit.*

[9] *Idem*.

En el presente trabajo se abordará el estudio del TRLPI y la LSE, y se procederá a su aplicación al caso de la herramienta Moriarty desarrollada por ITAINNOVA.

3. METODOLOGÍA

Teniendo en cuenta el interrogante planteado en este Trabajo Fin de Grado, para dar respuesta al mismo se utilizaran tres perspectivas de análisis: la doctrinal, sobre la base de estudios de diferentes juristas relacionados con la protección del *machine learning*; la jurisprudencial, mediante el análisis de los pronunciamientos de los tribunales, y la normativa, mediante el análisis de la regulación vigente aplicable.

A la hora de seleccionar el material bibliográfico del que se ha partido para elaborar el presente trabajo, se ha tenido especial cuidado en elegir los que son adecuados para el objetivo perseguido, descartando aquellos con información desfasada o que hacían referencia a legislación derogada. No obstante, al entrar en vigor recientemente la LSE, se ha tenido que adoptar un enfoque crítico, puesto que tanto la doctrina como la jurisprudencia no hacen referencia a dicha regulación, sino a la anteriormente vigente.

El análisis de la normativa vigente aplicable ha sido pilar fundamental para el desarrollo del presente Trabajo Fin de Grado. Concretamente, al no existir una figura jurídica que regule las soluciones de *machine learning* en su conjunto, ha sido necesario analizar diversas normativas en función de los distintos componentes del *machine learning*. Por un lado, se analizará la novedosa LSE en lo relativo a la protección de algoritmos como secretos empresariales y, por otro lado, en lo relativo al *big data,* se estudiará los elementos más relevantes del derecho "sui generis" sobre bases de datos regulado en el TRLPI.

Una vez estudiadas las figuras jurídicas aplicables a la protección del *machine learning*, se ha localizado jurisprudencia para conocer cuál es la postura de los tribunales en relación con dichas figuras y, por tanto, cuál es la protección jurídica en los casos concretos. La perspectiva de investigación ha sido deductiva ya que una vez conocida la regulación del ámbito general, la hemos aplicado al caso concreto, yendo de lo general a lo particular.

II. MACHINE LEARNING

1. CONCEPTO

El concepto de inteligencia artificial es fruto de unas conferencias que tuvieron lugar en 1956 en el Dartmouth College, en Hanover (New Hampshire, Estados Unidos). Los investigadores allí reunidos discutieron acerca de la posibilidad de construir máquinas que no se limitaran a hacer cálculos prefijados sino operaciones genuinamente "inteligentes"[10].

En 1990, Kurzweil definió la inteligencia artificial como «el arte de desarrollar máquinas con capacidad para realizar funciones que cuando son realizadas por personas requieren de inteligencia»[11]. Posteriormente, Rich y Knight la definieron como «el estudio de cómo lograr que los computadores realicen tareas que, por el momento, los humanos hacen mejor»[12].

Dentro de la inteligencia artificial se han desarrollado diferentes subdisciplinas, entre las que destaca el *machine learning*, la cual tiene como objetivo el lograr que las máquinas sean capaces de aprender, mediante la creación de programas o algoritmos con capacidad para generalizar un comportamiento concreto frente a determinados estímulos, a partir de una información proporcionada a modo de entrenamiento, que sirve para retroalimentar al sistema[13]; es decir, su objetivo es crear programas que permitan obtener patrones generalizables a través de la información no estructurada suministrada mediante ejemplos (*big data*)[14].

La revolución tecnológica ha causado que cada ser humano sea una fuente de generación de datos sobre los intereses, valores y preferencias de consumo que se registran a través de las redes sociales como Instagram, Facebook, WhatsApp,

---

[10] COLLE, R., *Algoritmos, grandes datos e inteligencia en la red. Una visión crítica.* Universidad de Alicante, España, 2017, pág 7.

[11] KURZWEIL, R., *The Age of Intelligent Machines,* The MIT press Cambridge, MA, USA, 1990.

[12] RICH, E y KNIGHT, K., *Artificial Intelligence,* McGraw Hill, 1991, pág. 3.

[13] GARCIA DEL POLLO, R., y GARCÍA, S., Implicaciones legales del machine learning, Revista Actualidad Mercantil, Tirant Lo Blanch, 2019, pág. 459.

[14] *¿Qué es Machine Learning?,* Artículo de Instituto Internacional Español de Marketing Digital (IIEMD). Disponible en: https://iiemd.com/machine-learning/que-es-machine-learning [Consulta 26/03/2019]

LinkedIn, Twitter, Pinterest, entre otros[15]. Diariamente se generan 2.5 exabytes de datos y se estima que para el año 2020, este volumen de información se habrá multiplicado 40 veces[16]. Los datos recopilados en internet por las empresas se acumulan en grandes bases de datos, que, en su conjunto, dada su magnitud, han pasado a llamarse *"big data"*.

Como ya se ha apuntado arriba, las capacidades humanas no son adecuadas para la explotación del *big data*. Se necesitan máquinas, máquinas capaces de aprender. La base del funcionamiento del *machine learning* son los algoritmos, secuencias de órdenes que conforman la base de la programación de los ordenadores y que permiten resolver problemas concretos. Concretamente, permiten la identificación de patrones complejos en grandes volúmenes de datos[17].

De forma simplificada, el *big data* proporciona una gran cantidad de información que permite que el algoritmo se "entrene" y que aprenda de patrones, relaciones y circunstancias del pasado. Una vez que el modelo este entrenado, se le puede proporcionar nueva información para que haga predicciones en función de los conocimientos que extrajo de los datos de entrenamiento[18].

Por ejemplo, imaginemos que queremos construir un algoritmo que nos permita detectar si un tumor es benigno o maligno en base a ciertas características del mismo. Para ello, tenemos a disposición una gran base de datos donde se recoge las características (I_n) de miles de tumores, así como su diagnóstico (0_n). Toda esa gran cantidad de información permite al algoritmo entrenarse en la identificación de tumores malignos y benignos. De forma que cuando el algoritmo este suficientemente entrenado, podrá hacer una predicción bastante fiable sobre las características de un nuevo tumor (I), del cual no

---

[15] UNIDAD DE INTELIGENCIA DE NEGOCIOS, *Machine Learning: Inteligencia que está transformando el mundo,* México, 2019, pág. 6. Disponible en: http://mim.promexico.gob.mx/work/models/mim/templates-new/Publicaciones/Notas/Machine-Learning.pdf [Consulta 26/03/2019]

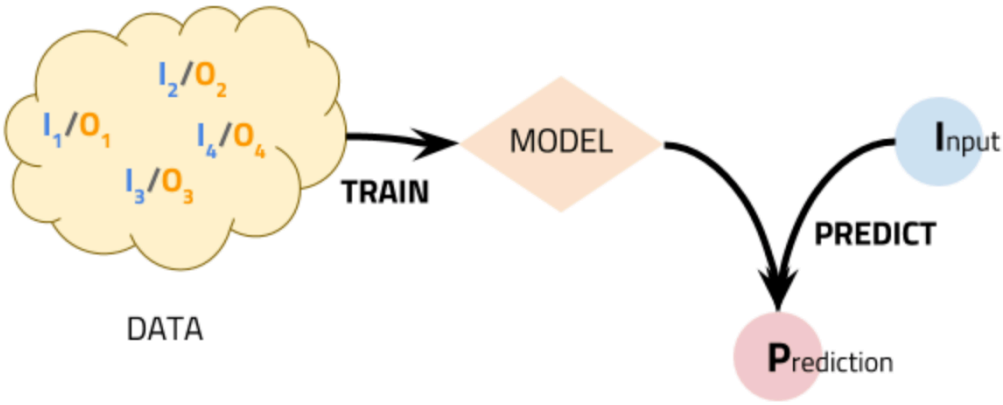
[16] OECD, Data Driven Innovation: Big Data for Growth and Well-Being, 2015.

[17] *¿Qué es Machine Learning y cómo se usa en Big Data?* Artículo de Universia España, 2017. Disponible en: http://noticias.universia.es/ciencia-tecnologia/noticia/2017/09/12/1155659/machine-learning-como-usa-big-data.html [Consulta 26/03/2019]

[18] ZAFORAS, M.., *"Machine Learning for dummies",* 2017. Disponible en: https://www.paradigmadigital.com/techbiz/machine-learning-dummies/ [Consulta 24/04/2019] citando a MUELLER, J., y MASSARON, L., *"Machine Learning for dummies",* John Wiley & Sons Inc, 2016.

sabemos si es benigno o maligno. En el siguiente gráfico se muestra una representación del modelo descrito[19].

Gráfico 1: Representación de un modelo de *machine learning.*



Fuente: Manuel Zaforas, 2017.

En conclusión, lo relevante del *machine learning* es que los algoritmos, entrenados mediante el análisis de los datos proporcionados por el *big data*, son capaces de catalogar nuevos resultados o incluso hacer predicciones. Basan su funcionamiento en una experiencia o conocimiento previo que los orienta en sus decisiones, logrando la aplicación de esta tecnología en múltiples áreas como la educativa, sanitaria, empresarial, entre otras[20].

2. PROBLEMÁTICA JURÍDICA

En la última década se ha producido un desarrollo extraordinario de nuevas tecnologías de la información, internet y digitalización que han revolucionado el panorama social y económico. Tanto es así, que algunos economistas han empezado a llamar a este fenómeno cómo la cuarta revolución industrial o la "industria 4.0"[21]. Parte de este gran

[19] ZAFORAS, M., ., *"Machine Learning for dummies"... op. cit.*

[20] *¿Qué es Machine Learning y cómo ... op. cit.*

[21] SCHWAAB, K., *La cuarta revolución industrial,* Debate, World Economic Forum, Madrid, 2016. Pág. 12-17.

desarrollo se debe a la implementación diaria de la inteligencia artificial y de sus componentes, el *big data* y los algoritmos[22].

Sin embargo, el *machine learning* supone un elevado coste de inversión puesto que, por un lado, es necesario elaborar y/o adquirir una base de datos suficientemente grande para poder obtener información relevante y, por otro lado, es necesario desarrollar un algoritmo lo suficientemente complejo para simplificar la información. Esta inversión se puede ver desalentada debido a la inseguridad jurídica en cuanto a su protección y a los riesgos crecientes derivados de la globalización, de la creciente externalización de los servicios, del mayor uso de tecnologías de la información y de la comunicación que contribuyen a aumentar el riesgo de robo, copia no autorizada, espionaje económico, entre otros (véase Preámbulo, LSE).

La inseguridad jurídica en cuanto a su protección se debe a la reciente actividad regulatoria del legislador y a que difiere para cada uno de sus componentes: *big data* y algoritmos.

a) En relación con el *big data*, el 1 de abril de 1998 entró en vigor la Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos[23] (en adelante, DBD), la cual, en concreto, en sus arts. 7 a 11, vino a colmar una laguna existente en todas las legislaciones de los países comunitarios. El Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el TRLPI resultaría, consiguientemente, modificado por la Ley de 5/1998[24]. En la mencionada normativa se prevén dos formas de protección para las bases de datos: el derecho de autor y el derecho "sui generis".

En relación con el primero de ellos, el legislador atribuye la tutela prevista por el derecho de autor a las bases de datos en sí mismas, esto es, con independencia de sus contenidos en función de la selección y sistematización de aquéllos, lo cual constituye una creación intelectual original propia del autor. Se protege, por tanto, la forma

---

[22] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos. Big data, desestructuración e inteligencia artificial* de Nuevos desafíos para el Derecho de Autor: robótica, inteligencia artificial, tecnología, director: NAVAS NAVARRO, S., Reus Editorial, Madrid, 2019. Pág. 183.

[23] Publicado en: «BOE» núm. 57, de 7 de marzo de 1998, páginas 7935 a 7940. Referencia: BOE-A-1998-5568

[24] VIVAS, T., *La tutela "sui generis" de las bases de datos,* Revista de Derecho Patrimonial, 2008, Núm. 21, pág. 159.

personal del autor de estructurar y disponer el contenido de la base de datos, pero no el propio contenido ni tampoco el *software* que permite la utilización de aquélla *ex* art. 12.3 LPI [25]. En relación con Moriarty, el contenido del *big data* utilizado por los algoritmos para hacer predicciones no ha sido estructurado ni dispuesto de una forma original por los trabajadores de ITAINNOVA por lo que no presenta la altura creativa suficiente para poder ser protegido por derechos de autor.

Por el contrario, el derecho "sui generis" protege, según dispone el art. 133 TRLPI, «la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza su fabricante ya sea de medios financieros, empleo de tiempo, esfuerzo, energía u otros de similar naturaleza, para la obtención, verificación, o presentación de su contenido». De esta forma, el legislador otorga un derecho al fabricante de una base de datos en cuanto inversor de cantidades ingentes de dinero y esfuerzo, concediéndole una ventaja empresarial para competir en el mercado al margen completamente de su personalidad creativa[26].

En el presente Trabajo de Fin de Grado nos centraremos en el análisis del derecho "sui generis" debido a que las bases de datos utilizadas por ITAINNOVA en sus proyectos de *machine learning* no pueden ser protegidas por derecho de autor.

b) En relación con los algoritmos, actualmente no existe una regulación jurídica especifica que los proteja debido a las dificultades que atraviesa el legislador para adaptarse a las nuevas tecnologías que se transforman y renuevan constantemente. Además, cómo se detalla a continuación, la protección del algoritmo ha sido expresamente excluida del amparo de ciertas normativas.

En lo relativo a la protección ofrecida por la TRLPI, dentro de las obras y títulos originales que dan lugar al derecho de autor se encuentran los programas de ordenador. Sin embargo, en el considerando decimocuarto de la Directiva 91/250/CEE, del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de los programas de ordenador [27], se estableció que «en la medida en que la lógica, los algoritmos y los lenguajes de programación abarquen ideas y principios, estos últimos no están

---

[25] VIVAS, T., *La tutela "sui generis" ... op. cit.,* pág. 162.

[26] *Ibídem*, págs. 162 y 164"

[27] Publicado en: «DOCE» núm. 122, de 17 de mayo de 1991, páginas 42 a 47. Referencia: DOUE-L-1991-80581

protegidos con arreglo a la Directiva» y, por tanto, no están protegidos por el derecho de autor. Tal postura ha sido mantenida por el TJUE en sus sentencias de 2 de mayo de 2012, en el asunto C-406/10 referente al caso SAS *Institute Inc vs World Programming*[28], y de 3 de julio de 2012, en el asunto C-128/11 caso *UsedSoft GmbH vs Oracle Internacional Corp*[29].

En lo relativo a la Ley 24/2015, de 24 de julio, de Patentes[30], en el art. 4.4 se recogen una serie de supuestos que quedan excluidos de su protección por no ser invenciones. Uno de ellos son los métodos matemáticos. La Oficina de Patentes Europea, en diversos pronunciamientos[31], ha considerado que los algoritmos son métodos matemáticos y como consecuencia, ha denegado su patentabilidad. Ello, sin perjuicio de que se puedan patentar los algoritmos cuando constituyan una parte inseparable de la solución técnica susceptible de ser patentada[32]. Sin embargo, los algoritmos desarrollados sobre el *software* Moriarty no constituyen una parte inseparable puesto que pueden ser utilizados desde cualquier equipo informático por lo que, en consecuencia, no pueden ser patentados. Además, es necesario tener en cuenta que el derecho de patente exige la publicación de la regla técnica en que consiste invención, lo que supondría la publicación del algoritmo en contra de lo intereses de sus desarrolladores[33].

A pesar de descartar los dos sistemas anteriores, el algoritmo puede protegerse en el ordenamiento jurídico español mediante la figura del secreto empresarial, siempre y cuando cumpla los requisitos establecidos por la legislación y la jurisprudencia.

---

[28] ECLI:EU:C:2012:259

[29] ECLI:EU:C:2012:407

[30] Publicado en: «BOE» núm. 177, de 25 de julio de 2015. Referencia: BOE-A-2015-8328

[31] Las Directrices para el examen de la OEP "*Guidelines for Examination in the EPO*, Part. G- Chapter II-6 y ss, november 2016", establecieron que, para que un software pueda acceder a la protección de la oficina de patentes, es necesario que tenga consideraciones técnicas más allá del mero hallazgo de un algoritmo que desarrolle algún proceso. Pues en caso contrario, no tendrá el carácter técnico necesario para poder ser protegido. Disponible en: https://www.epo.org/law-practice/legal-texts/html/caselaw/2016/e/clr_i_d_9_1_8.htm [Consulta 28/03/2019].

[32] FERNÁNDEZ, M, *La protección de la Inteligencia Artificial determina el desarrollo tecnológico,* Bird&Bird, 2019. Disponible en: http://www.legaltoday.com/actualidad/noticias/la-proteccion-de-la-inteligencia-artificial-determina-el-desarrollo-tecnologico [Consulta 14/05/2019].

[33]SAIZ GARCÍA, C., Las obras creadas por sistemas de inteligencia artificial y su protección por el derecho de autor, Revista para el análisis del Derecho INDRET, Nº1, 2019, Barcelona. Disponible en: http://www.indret.com/pdf/1446.pdf [Consulta 28/03/2019].

Hasta la reciente entrada en vigor de la LSE, el concepto de secreto empresarial no se encontraba definido en el ordenamiento español, recurriendo los tribunales a la definición recogida en el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (en adelante, ADPIC). De conformidad con el acuerdo, «se considera secreto empresarial toda información que sea secreta, que tenga un valor comercial por ser secreta y que haya sido objeto de medidas razonables para que permanezca en secreto»[34].

Tal definición se recogió en la DSE. El fin de la Directiva era armonizar la legislación de los Estados miembros con el objetivo de establecer un nivel suficiente y comparable de reparación en todo el mercado interior en caso de apropiación indebida de secretos empresariales. Concretamente, la explotación o divulgación no autorizada de un algoritmo considerado como secreto empresarial permitiría al titular del mismo el ejercicio de acciones legales, en virtud del art. 13 LCD (véase Preámbulo LSE).

El 13 de marzo de 2019 entró en vigor la LSE, la cual aborda el mandato de transposición de la DSE y, con el fin de incorporarla a nuestro ordenamiento jurídico, busca mejorar la eficacia de la protección jurídica de los secretos empresariales contra la apropiación indebida en todo el mercado interior completando la regulación anterior desde una perspectiva sustantiva y, especialmente, procesal (véase Preámbulo LSE).

En conclusión, en el presente trabajo se analizarán los diversos mecanismos jurídicos de protección del *machine learning*. En primer lugar, se estudiará la protección que el TRLPI brinda para el *big data*. En segundo lugar, se analizará la protección de los algoritmos como secreto empresarial regulada en la LSE. Por último, se obtendrán conclusiones útiles sobre qué herramientas jurídicas, presentes en la legislación española, utilizar para proteger el proyecto Moriarty de la entidad ITAINNOVA.

[34] *Algoritmo o software: ¿dónde reside mi propiedad intelectual?*. Artículo de ECIJA 16/11/2016. Disponible en: https://ecija.com/algoritmo-software-donde-reside-propiedad-intelectual/ [Consulta 26/03/2019]

III. PROTECCIÓN DEL BIG DATA.

1. CONCEPTO DE BIG DATA

Uno de los principales cimientos de la llamada cuarta revolución industrial es la generación, recopilación y tratamiento de información a gran escala, también conocida como *big data.* Existen diversas definiciones de *big data*, pero, en palabras de Romeu I Cónsul, la mayoría de ellas parecen coincidir en que se trata de un sistema o conjunto de recursos tecnológicos que tienen como objetivo la recolección, almacenamiento y tratamiento de datos a gran escala, mediante el uso de diferentes técnicas de computación.

La principal utilidad del *big data* es el análisis de los datos mediante algoritmos y métodos matemáticos, con el fin de encontrar correlaciones entre los datos que permitan detectar tendencias, patrones o pautas de conductas[35]. Un artículo de investigación de 2001, escrito por Doug Laney de Gartner, definió las "tres Vs" del *big data* de la siguiente forma[36]:

- Volumen: El proyecto de *big data* se basa en el tratamiento de grandes cantidades de datos sobre un tema dado[37]. El origen de esos datos se encuentra en el incremento del uso y desarrollo de plataformas virtuales cómo Facebook, donde se suben más de 10 millones de fotos cada hora y se pulsa el botón de "me gusta" tres mil millones de veces diarias, o Google, que procesa más de 24 petabytes de datos al día, entre otros[38].
- Variedad: A diferencia de las tradicionales bases de datos que han funcionado como un sistema estructurado de datos homogéneos, el *big data* gestiona grandes cantidades de datos con diferentes formatos y fuentes (texto, imágenes, hojas de Excel, entre otros) y, de esta forma, utiliza bases de datos desestructuradas con formatos mucho más flexibles[39].

---

[35] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 188.

[36] MAYER-SCHÖNBERGER, V., *Big data. La revolución de los datos masivos,* (Antonio Iriarte, trad.), Turnes Publicaciones, Madrid, 2013. Pág. 639.

[37] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 189..

[38] MAYER-SCHÖNBERGER, V., *Big data. La revolución de … op. cit.,* pág. 27 y 28..

[39] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 189..

- Velocidad: El *big data* trabaja a tiempo real de forma que los datos se actualizan automáticamente[40].

2. CONCEPTO DE BASE DE DATOS EN EL TRLPI Y SU PROBLEMÁTICA EN RELACIÓN CON EL BIG DATA.

La DBD definió por primera vez, *ex* art. 1.2, el concepto de base de datos el cual fue recogido en el artículo 12.2 TRLPI cómo «las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma».

La definición fue muy criticada por la doctrina[41] por considerarla insuficiente lo que llevó a que, en el año 2009, el TJUE se pronunciará en la sentencia de 5 marzo 2009[42], asunto C-545/07, *Apis-Hristovich EOOD vs Lakord AD*, estableciendo que el concepto de base de datos debía de ser interpretado con gran amplitud. Concretamente, para que una recopilación de información sea considerada base de datos, es suficiente con que reúna los requisitos de disposición sistemática o metódica y de accesibilidad individual de los datos contenidos en ella[43]. De hecho, la sentencia del mismo Tribunal de 9 de noviembre de 2004 [44] , asunto C-444/02, *Fixtures Marketing vs Organismos prognostikon agonon podosfairou AE (OPAP)*, apartados 29 a 32, permite diseccionar los dos requisitos básicos, de tal forma que la existencia de una base de datos está supeditada a la concurrencia de cuatro requisitos, algunos de ellos, problemáticos con la naturaleza del *big data.*

El primero de ellos determina que la existencia de una base de datos requiere la recopilación de elementos independientes. Este requisito no plantea problemas en relación con el *big data* debido a que, por definición, está formado por datos masivos independientes unos de otros.

---

[40] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 189..

[41] Diferentes juristas elaboraron sus propias definiciones de bases de datos. Por ejemplo, Braustein define las bases de datos como «colecciones o compilaciones de registros, organizadas para facilitar el acceso a ellas o la recuperación de sus datos».

[42] ECLI:EU:C:2009:132

[43] Sentencia del TJUE de 1 de marzo de 2012, asunto C-604/10, *Football Dataco Ltd y otros vs Yahoo UK Ltd.* y otros, apartado 26. ECLI:EU:C:2012:115

[44] ECLI:EU:C:2004:697

El segundo requisito hace referencia a que, en la base de datos, debe existir una disposición sistemática o metódica de los elementos recopilados. Este requisito es problemático debido a que en el *big data* la información es masiva, lo que dificulta su gestión humana y, por tanto, la disposición sistemática o metódica de la misma. Hay que tener en cuenta que la DBD fue aprobada en el año 1996, cuando todavía no se había desarrollado la tecnología *big data* y no se generaban datos masivos con el volumen, la variedad y la velocidad del momento presente. El objetivo de la Directiva fue regular las bases de datos que se utilizaban en aquel momento, las cuales, estaban formadas por información limitada que permitía su gestión manual y, por tanto, su disposición sistemática y metódica.

El tercer requisito hace referencia a que exista algún instrumento técnico, cómo un índice, sumario, plan o modo de clasificación, que permita la localización de cualquier elemento independiente. Cómo se ha expuesto en el párrafo anterior, el cumplimiento de este requisito era habitual en bases de datos utilizadas cuando la DBD fue aprobada. Sin embargo, la gran cantidad de datos manejados por el *big data* hacen que, actualmente, sea de imposible cumplimiento.

Por último, se exige la accesibilidad individual a los elementos recopilados. Este requisito no plantea problemas en relación con el *big data* puesto que se puede acceder individualmente a todos los datos.

Por todo lo anterior, el *big data* no se identifica con el concepto de base de datos regulado en la DBD, sino que, engloba mucho más[45], lo que ha provocado que, a nivel europeo, numerosos expertos hayan alertado de que no existe una regulación adecuada del *big data*, ni de cuáles son los derechos que se pueden ver afectados o cuales son los mecanismos jurídicos para su protección[46].

En 2005, se realizó la primera evaluación de la implementación de la DBD, donde quedó en evidencia el retraso europeo en relación al desarrollo de mercados punteros de

---

[45] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 192..

[46] AZUAJE PIRELLA, M., y FINOL GONZÁLEZ, D., Big Data, algoritmos y propiedad intelectual, Revista Anuario de Propiedad Intelectual, Nº 2016, 2017, pág. 257-275 citado por ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 191..Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6150503

bases de datos como consecuencia del escaso impacto que la normativa había tenido sobre la inversión, situación que no ha mejorado en la actualidad[47].

Así, actualmente, el legislador europeo se encuentra en pleno proceso de restructuración de varias Directivas que afectan a los derechos de autor; entre ellas la DBD[48]. De hecho, tras un intento fallido en julio de 2018, el Parlamento europeo aprobó el pasado 26 de marzo el texto revisado del proyecto de Directiva presentado por la comisión para la reforma de la normativa sobre derechos de autor en el mercado único digital, del que se tratará *infra*.

A pesar de todo lo anterior, la DBD y el TRLPI todavía no han sido modificadas, siendo, a pesar de los problemas que plantean, las únicas normativas protectoras del *big data* en la actualidad. Es por ello, que en los siguientes apartados, se analizará el derecho "sui generis" y su posible aplicación al *big data*[49].

3. EL DERECHO SUI GENERIS SOBRE LA BASE DE DATOS.

3.1 Objeto de la tutela "sui generis"

A) La inversión sustancial

Tal y como establece el art. 133 TRLPI, reproducido *supra*, el derecho "sui generis" protege la inversión sustancial que ha realizado el fabricante de una base de datos para obtener, verificar o presentar su contenido. Por tanto, la noción del derecho "sui generis" se explica en función de la importancia de la inversión que se ha realizado para elaborar la base de datos, independientemente de la altura creativa del resultado[50]. En consecuencia, cualquier base de datos que haya sido elaborada mediante una gran inversión (dinero, tiempo, esfuerzo) sustancial brindará a su fabricante la protección específica del derecho "sui generis"[51].

---

[47] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 191..

[48] *Ibídem*, pág. 194".

[49] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 194..

[50] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017, pág. 1541.

[51] BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos: génesis, evolución y perspectivas,* Aranzadi-Thomson Reuters, Cizur Menor, 2009, pág. *117*

Surge por tanto la necesidad de estudiar qué se entiende por inversión sustancial. Al respecto, la Directiva aclaró que el carácter sustancial de una inversión se evaluará tanto desde el punto de vista cuantitativo como cualitativo[52].

Inversión cualitativamente sustancial es aquella que tiene importancia para la actividad mercantil productiva en la que produce[53] como, por ejemplo, cuando se destinan recursos para el uso profesional especializado o un *software* específico para el tratamiento de datos[54].

La inversión cualitativamente sustancial deberá determinarse en función de la proporción que representen los recursos gastados en la confección de un cierta base de datos con respecto al total de recursos de los que dispone el fabricante de la misma para la actividad[55]. Para ello, no habrá que tener sólo en cuenta los recursos económicos empleados, sino también, el empleo de esfuerzo, energía y tiempo (véase cdo. 40 DBD).

Así las cosas y dado que no existe ningún parámetro objetivo que nos permita determinar el concepto de «inversión sustancial». será, en última instancia, el juzgador quien, en cada caso concreto, deba decidir cuándo la inversión, en términos cuantitativos y/o cualitativos, realizada por el fabricante de la base de datos es lo suficientemente «sustancial» como para ser merecedora de la tutela «sui generis» dispensada por la TRLPI[56].

Sin perjuicio de lo anterior, ha de ponerse de relieve que ITAINNOVA, para desarrollar su proyecto Moriarty, ha invertido grandes cantidades de recursos, utiliza equipamiento exclusivo y cuenta con una plantilla de trabajadores ocupados exclusivamente en gestionar el *big data* y desarrollar algoritmos que permitan analizarlo. Es por ello que puede afirmase que, en principio, ITAINNOVA ha realizado una inversión sustancial en la elaboración de la base de datos utilizada en su proyecto Moriarty, cumpliéndose este requisito.

---

[52] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1541.

[53] BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos… op. cit.,* pág. 120..

[54] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 200..

[55] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1542..

[56] VIVAS, T., *La tutela "sui generis" … op. cit.,* pág. 166..

B) Objeto de la inversión: obtener, verificar o presentar el contenido.

Para que una base de datos sea protegida por el derecho "sui generis" es necesario que la inversión sustancial se realice con el objetivo de obtener, verificar o presentar el contenido. Tras la entrada en vigor de la DBD, en los países europeos, surgieron numerosas sentencias que mostraron una clara diversidad en relación a cómo interpretar tales términos[57].

En fecha de 9 de noviembre de 2004 el TJUE emitió unos trascendentales veredictos en los asuntos C-46/02[58], C-203/02[59], C-338/02[60] y C-444/02[61], acerca de la interpretación de la DBD. Las cuatro decisiones judiciales concluyeron que, a pesar de haberse realizado inversiones sustanciales, tanto desde un punto de vista cuantitativo como desde un punto de vista cualitativo, las bases de datos analizadas no eran dignas de la tutela "sui generis" y, además, ayudaron a esclarecer los conceptos de obtención y verificación y presentación del contenido de una base de datos.

Tales conceptos han terminado de ser perfilados por la doctrina. Concretamente, Palau Ramírez y Palao Moreno[62] los definen de la siguiente forma:

- El concepto de inversión destinada a la obtención del contendido de una base de datos debe entenderse en el sentido de que se refiere a los recursos dedicados a la búsqueda de datos ya existentes y a su recopilación en dicha base.
- El concepto de inversión destinada a la verificación del contenido de la base de datos debe entenderse en el sentido de que se refiere a los recursos que se dedican al control de la exactitud de los datos buscados para mantenerlos depurados y actualizados.
- El concepto de inversión destinada a la presentación del contenido de la base de datos debe entenderse en el sentido de que se refiere a los recursos consagrados a la disposición sistemática o metódica de los datos insertos en la base, así como

---

[57] BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos… op. cit.,* pág. 219..

[58] ECLI:EU:C:2004:694

[59] ECLI:EU:C:2004:695

[60] ECLI:EU:C:2004:696

[61] ECLI:EU:C:2004:697

[62] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1545..

a la organización de su accesibilidad individual, que confieren a la base su función de tratamiento de la información.

Una de las características más problemáticas del *big data* es la desestructuración de la información cómo consecuencia del manejo de grandes volúmenes de datos. De hecho, grandes empresas interesadas en el *machine learning* están invirtiendo en tecnologías más aptas para trabajar con bases de datos desestructuradas, pues permiten una mayor flexibilidad y se adaptan mucho mejor a las finalidades de los proyectos de *machine learning* que las bases de datos tradicionales. Ello no quita que los creadores del *big data* no hayan realizado una inversión sustancial en la recopilación, verificación o presentación de los contenidos[63].

Sin embargo, los conceptos de obtención, verificación y presentación del contenido, definidos anteriormente, no se adaptan completamente a la naturaleza del *big data* debido a los siguientes motivos:

En relación con la inversión sustancial destinada a la obtención del contenido, se plantea el problema de si el derecho "sui generis" se aplica también a las bases de datos que se nutren de la información recibida por sensores o creadas por máquinas. Si bien es cierto que el TJUE afirmó que, toda inversión sustancial que recaiga sobre la obtención, verificación o presentación del contenido de una base de datos, estará protegida por el derecho "sui generis", muchos autores dudan si las bases de datos creadas por máquinas o sensores pueden llegar a estar protegidas[64].

En relación con la inversión sustancial destinada a la presentación del contenido, se plantea el problema de sí las bases de datos desestructuradas, donde no existe ningún tipo de orden dentro de los datos, quedarán amparadas por la normativa[65].

Centrándonos en el proyecto de ITAINNOVA, el instituto tecnológico aragonés ha realizado una inversión sustancial, tanto desde el punto de vista cualitativo (por ejemplo, uso de *software* específico para la obtención y tratamiento de los datos) cómo cuantitativo (por ejemplo, la existencia de trabajadores dedicados exclusivamente al

---

[63] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 208..

[64] Comisión Europea, Study in support of the evaluation of directive 96/6/EC on the legal protection of databases", 2018, Directorado-General de Redes de Comunicaciones, Contenido y Tecnología. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1/language-en/format-PDF/source-92832355 [Consulta 01/04/2019]. Pág 111-112.

[65] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 200..

proyecto Moriarty) destinada a la obtención, verificación y presentación del contenido de la base de datos utilizada en el proyecto cómo se detalla a continuación.

En relación con la obtención del contenido de la base de datos utilizada en el proyecto, ITAINNOVA ha desarrollado herramientas que le permiten capturar los datos de fuentes cuantitativas (redes sociales, páginas web, entre otras) y cualitativas (sensores meteorológicos, maquinaria, imágenes, entre otras) en función de las necesidades de los proyectos a los que se aplica la tecnología Moriarty.

En relación con la verificación de los datos contenidos en la base de datos utilizada en el proyecto, los trabajadores encargados de controlar la tecnología Moriarty dedican parte de su tiempo a filtrar la información con el objetivo de mejorar la precisión del algoritmo.

Por último, en relación con la presentación del contenido de la base de datos, los trabajadores dedican más o menos tiempo a estructurar de forma lógica la información dependiendo de cada proyecto y de la necesidad de elaborar informes y generar modelos de inteligencia.

3.2. La titularidad del derecho

La DBD alude, en su artículo 7.1, al fabricante de la base de datos como beneficiario inicial del derecho "sui generis", y, sin embargo, no ofreció una definición de lo que debe entenderse por fabricante de base de datos: si quien toma la iniciativa, quien asume el riesgo o quien hace una inversión sustancial en la creación de la base de datos[66]. Esto ha llevado a la transposición de la Directiva en diferentes términos, lo que supone una gran inseguridad jurídica[67].

Centrándonos en España, el legislador español ha optado por definir al fabricante de datos como «la persona natural o jurídica que toma la iniciativa y asume el riesgo de efectuar las inversiones sustanciales orientadas a la obtención, verificación o presentación de su contenido» (art. 133.3.a) TRLPI). De esta forma, el titular del derecho "sui generis" es, siempre, el que toma la iniciativa y asume el riesgo de la

[66] Comisión Europea, Study in support of the evaluation of directive 96/6/EC on the legal protection of databases", 2018, Directorado-General de Redes de Comunicaciones, Contenido y Tecnología. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1/language-en/format-PDF/source-92832355 [Consulta 01/04/2019] Pág. 31-32.

[67] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 204..

operación, independientemente, de que la inversión sustancial de recursos, tiempo, esfuerzo, entre otros, haya sido realizada por terceras personas, caso común en el ámbito laboral.

En relación con el proyecto de ITAINNOVA, la entidad aragonesa es la que decidió apostar por el desarrollo de un proyecto de *machine learning* así cómo asumir el riesgo de la operación por lo que, de acuerdo con el TRLPI, es el titular del derecho "sui generis". Todo ello, con independencia de que la inversión sustancial de tiempo y recursos la hayan realizado mayormente los trabajadores que dedican su jornada laboral al desarrollo de la herramienta Moriarty.

Por otro lado, en la DBD y en el TRLPI no se aclaró quien debe de ser el titular del derecho "sui generis" para los casos en los que son varias personas las que asumen el riesgo, toman la iniciativa o invierten esfuerzos o capital en la creación de la base de datos. Esta escasa determinación de quién es el fabricante plantea bastante problemas en entornos de creación de *big data* donde es muy común la existencia de varios participantes[68].

En conclusión de lo *supra* expuesto, puede afirmarse que el *big data* contenido en la base de datos, teniendo en cuenta la necesidad de hacer una interpretación conforme a esta nueva realidad de las normas contenidas en el TRLPI, reúne los requisitos para su protección como derecho "sui generis", siendo ITAINNOVA el sujeto titular de contenido de este derecho.

3.3. Contenido del derecho "sui generis"

El derecho "sui generis" permite al fabricante de la base de datos «prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, siempre que la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo» (art. 133.1, párr. 2.º, TRLPI).

El propio artículo, siguiendo la DBD, define la extracción como la transferencia permanente o temporal de la totalidad o de una parte sustancial del contenido de una base de datos a otro soporte cualquiera que sea el medio utilizado o la forma en que se

[68] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 205...

realice[69], pudiendo ocurrir, por ejemplo, mediante la descarga o copiado del contenido de la base o mediante la creación de una nueva base de datos a consecuencia de su consulta reiterada[70].

Por otro lado, la reutilización es a tenor del artículo 133.3, c) TRLPI «toda forma de puesta a disposición del público de la totalidad o de una parte sustancial del contenido de la base mediante la distribución de copias en forma de venta u otra transferencia de su propiedad o por alquiler, o mediante transmisión en línea o en otras formas».

La expresión «toda forma» es una formula indeterminada que permite no sólo los modos expresamente mencionados, sino también otros ya existentes hoy en día o que se inventen en el futuro. Por otra parte, «puesta a disposición del público» consiste en el ofrecimiento al público de la base de datos para que este acceda a su contenido careciendo de relevancia que la oferta tenga éxito o no[71].

De este modo, se otorga al titular de la base de datos un *ius prohibendi* con relación a la extracción y/o la reutilización de la totalidad o de una parte sustancial del contenido de la base de datos. Nuevamente surge un problema interpretativo acerca del carácter «sustancial» de la parte de la base de datos extraída y/o reutilizada[72].

La jurisprudencia establecida por el TJUE en el asunto C-545/07[73] determinó que el concepto de "parte sustancial" ha de evaluarse respecto del contenido total, bien de modo cuantitativo, atendiendo al volumen de datos extraídos o reutilizados, o bien cualitativo, atendiendo a la magnitud de la inversión destinada a la obtención, verificación o presentación del contenido extraídos o reutilizado, independientemente del volumen que éste represente cuantitativamente[74].

Así pues, ITAINNOVA, cómo titular del derecho "sui generis", puede prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial de la base de datos

---

[69] La calidad de los datos transferidos carece de relevancia. Así existe una extracción aun cuando la transferencia se realice con un escáner de mala calidad o cuando al teclear los datos parte de ellos se vean alterados. BOUZA, M., *El derecho sui generis del fabricante de bases de datos* pág. 201 citando a BUSCH, C., *La protección penal de los derechos de autor en España y Alemania,* Cedecs, Barcelona, 1995, pág 130.

[70] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 202..

[71] BOUZA, M., *El derecho sui … op. cit.,* pág. 207..

[72] VIVAS, T., *La tutela "sui generis" … op. cit.,* pág. 167..

[73] ECLI:EU:C:2009:132

[74] BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos… op. cit.,* pág. 227..

utilizada en la herramienta de inteligencia artificial Moriarty, siempre que la obtención, verificación o la presentación del contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo.

Por el contrario, en virtud del art. 134 del TRLPI, el fabricante no podrá impedir al usuario legítimo las extracciones o reutilizaciones de partes insustanciales de su contenido independientemente del fin al que se destine[75]. La DBD no incluyó más precisiones acerca de quién es el usuario legítimo lo que ha generado una gran inseguridad jurídica a nivel europeo debido a que los Estados miembros han optado por fórmulas muy diversas, desde conceptos muy amplios hasta otros mucho más restrictivos que lo equiparan a usuario con licencia[76].

En el caso español, el legislador ha optado por no delimitar de forma precisa la figura de usuario legítimo. Autores cómo Palau Ramírez y Palao Moreno definen al usuario legitimo como aquella persona que teniendo acceso efectivo y jurídicamente reconocido a una base de datos es susceptible de resultar afectada por un poder de veto ejercitable por el fabricante, consistente bien en impedirle extracciones y/o reutilizaciones de partes sustanciales de una base que haya sido objeto de una inversión sustancial o bien de partes no sustanciales cuando tales actuaciones perjudiquen acreditadamente la explotación normal o lesionen injustificadamente los intereses legítimos del fabricante[77].

3.4. Duración del derecho.

La existencia del derecho "sui generis" supone el establecimiento de unos límites temporales al mismo. A este fin, el legislador introdujo el artículo 136 del TRLPI[78] que establece, en su primer apartado, que el derecho "sui generis" sobre una base de datos tiene como *dies a quo* el de la finalización de su proceso de fabricación y concluye

---

[75] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1559..

[76] Comisión Europea, Study in support of the evaluation of directive 96/6/EC on the legal protection of databases", 2018, Directorado-General de Redes de Comunicaciones, Contenido y Tecnología. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1/language-en/format-PDF/source-92832355 [Consulta 01/04/2019]. Pág. 11 y 15.

[77] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1560

[78] PÉREZ DE ONTIVEROS BAQUERO, C., *En relación con el derecho de autor* en Comentarios, Tecnos, 2ª Ed., pág. 598.

quince años después del 1 de enero del año siguiente a la fecha de finalización[79], sin que sea necesario cumplir con ningún requisito de inscripción, depósito o divulgación[80].

El apartado 2 del artículo 136 TRLPI establece un añadido con respecto al apartado anterior, al indicar que la puesta a disposición de la base de datos originará el nacimiento de un nuevo plazo de protección que se extenderá por quince años a contar desde el 1 de enero del año siguiente a la primera puesta a disposición del público, y ello sin perjuicio del tiempo ya trascurrido bajo el manto protector dispensado por el anterior apartado[81]. La puesta a disposición ha de ser efectiva siendo irrelevante si el público accede a la base o no y debe tener lugar antes de la expiración del periodo de quince años, puesto que si transcurre el plazo, no surgirá un nuevo periodo de protección[82].

Por tanto, la protección temporal del derecho "sui generis" sobre las bases de datos es muy amplia, debido a que puede alcanzar los 30 años en los casos en los que, en el día en el que fuera a vencer la tutela de una base de datos aun no difundida, su fabricante la pusiera a disposición del público. Numerosos expertos han criticado que este plazo es excesivamente largo y han propuesto disminuir su duración a 5 años, de esta forma, el máximo tiempo que podría el derecho "sui generis" proteger la inversión sustancial sería de 10 años[83].

Por último, el apartado 3 del artículo 136 TRLPI prevé que cualquier modificación sustancial, evaluada de forma cuantitativa o cualitativa, del contenido de una base de datos y, en particular, cualquier modificación sustancial que resulte de la acumulación de adiciones, supresiones o cambios sucesivos que conduzcan a considerar que se trata de una nueva inversión sustancial permitirá atribuir a la base resultante de dicha inversión un plazo de protección propio. Diversos autores[84] entienden que es posible la perpetuación de la protección del derecho "sui generis" mediante la sucesión de

---

[79] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1567..

[80] BERCOVITZ RODRIGUEZ CANO, R., Comentarios a la Ley de Propiedad Intelectual, Tecnos, 2007 3ª Ed, pág 25.

[81] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1567..

[82] BOUZA, M., *El derecho sui … op. cit.,* pág. 239..

[83] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 213..

[84] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1567 citando a BOVENVERG y CAMARA LAPUENTE.

inversiones sobre una base de datos siempre y cuando cumplan dos requisitos: que sean el resultado de una modificación sustancial de su contenido evaluada cuantitativamente o cualitativamente, y que tal modificación permita considerar que se trata de una nueva inversión sustancial. Concretamente, Bovenberg defiende que el derecho "sui generis" puede mantenerse a perpetuidad dado que puede ir siendo desarrollado al compás que cualquier modificación de la base de datos que requiera una inversión sustancial[85].

Este apartado plantea muchos problemas en relación con el *big data*, debido a que la información utilizada por esta nueva tecnología se renueva constantemente. Cómo se ha mencionado anteriormente, el origen de la información se encuentra en el desarrollo de internet y de las tecnologías de la información que permiten que cada aspecto de nuestras vidas sea susceptible de convertirse en un dato, ya no sólo nuestros datos identificativos, sino también, nuestras búsquedas en internet, las veces que entramos en una página web, nuestra ubicación, entre otros[86]. Por tanto, surge la problemática de determinar si la constante actualización de la información contenida en el *big data* supone una nueva modificación sustancial de la base de datos que permite atribuir a la base resultante de dicha inversión un plazo de protección propio.

Además, atendiéndonos a lo dispuesto en el art. 136.1 TRLPI, el derecho "sui generis" nace cuando se finaliza el proceso de fabricación de la base de datos. Por tanto, no surge en el momento de realizar la inversión, ni en el de la obtención, verificación o presentación del contenido. En relación con el *big data,* el problema surge en determinar cuándo se finaliza el proceso de fabricación puesto que la base de datos se actualiza constantemente.

Para solucionar toda esta problemática, la doctrina considera que es necesario un entendimiento dinámico de la sucesión de versiones de una misma base de datos que vayan surgiendo en el mercado, cada una de las cuales seguirá sus propias vicisitudes de manera independiente pudiendo existir varios derechos "sui generis" sobre las diferentes versiones existentes[87]. De esta forma, las consecutivas versiones surgidas de la actualización automática del *big data* serían independientes y darían lugar a diversos

---

[85] BOVENBERG, J.A. Should Genomocs Companies set up Data Base in Europe?. The EU Database protection Directive Revisited, EIPR, vol 23, nº8, agosto de 2001, pág. 365.

[86] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 186..

[87] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1570...

derechos "sui generis" sobre cada una de ellas con plazos de protección diferentes. Sin embargo, este enfoque plantea el problema de que el *big data* trabaja con datos masivos que, debido a las actualizaciones, no paran de crecer, por lo que, si se considera cada actualización como una nueva versión, a lo largo del tiempo existirían tantas versiones, susceptibles de ser protegidas por el derecho "sui generis", como datos actualizados.

Para evitar este problema, autores cómo Bouza López defienden que en estos supuestos se puede acudir a la ficción de que las bases se finalizan el 31 de diciembre de cada año protegiéndolas durante quince años tal y cómo estén en ese momento concreto[88]. De esta forma, en relación con el *big data* utilizado por ITAINNOVA, cada 31 de diciembre se finaliza una nueva versión, que incluye todas las actualizaciones realizadas durante el año, susceptible de ser protegida por el derecho "sui generis", durante 15 años.

3.5 Las acciones para la defensa del derecho "sui generis".

El derecho "sui generis" puede ser protegido por todos los mecanismos contemplados en el Libro III TRLPI. De esta forma, *ex* art.138 TRLPI, el titular del derecho "sui generis" puede instar la cesación de la actividad ilícita así como exigir una indemnización por los daños materiales sufridos[89]ante situaciones de extracción y/o reutilización de partes sustanciales de bases de datos.

La legitimación activa la ostenta ITAINNOVA, puesto que, tal y cómo se ha mencionado en epígrafes anteriores, es el titular del derecho "sui generis" sobre la base de datos utilizada en el proyecto Moriarty.

La legitimación pasiva frente a las acciones de cesación y de indemnización la ostenta quien infringe alguno de los derechos reconocidos en el TRLPI, es decir, quien realiza actos de extracción o de reutilización o actos contrarios a una explotación normal que lesionen injustificadamente los intereses del ITAINNOVA sin que tengan relevancia los elementos del culpa[90].

---

[88] BOUZA, M., *El derecho sui ... op. cit.,* pág. 236..

[89] Art. 138 TRLPI

[90] BOUZA, M., *El derecho sui ... op. cit.,* pág. 251.citando a CASTÁN PÉREZ GÓMEZ, A., en Comentarios, EDERSA, 4ºB, pág. 638-639

En relación con el plazo para ejercitar las acciones, las acciones de cesación prescriben a los seis años de la comisión de la infracción[91], con independencia de que el periodo de protección de quince años ya haya finalizado, mientras que la acción de indemnización prescribe a los cinco años contados desde el día en que se pudiera ejecutar; es decir, desde el momento en el que el perjudicado tiene conocimiento de la infracción y del carácter dañoso, aunque todavía no conozca la cuantía de los daños[92].

A continuación, voy a hacer una revisión de las principales acciones de cesación de las que puede disponer ITAINNOVA cómo titular del derecho "sui generis" sobre la base de datos utilizada en el proyecto Moriarty:

- Las letras a) y b) del artículo 139 TRLPI establecen que el cese de la actividad ilícita podrá comprender la suspensión de la actividad infractora y la prohibición de reanudarla. De esta forma se determina que determinados actos sólo pueden ser realizados por el titular del derecho y se condena al autor de la infracción a una obligación de no hacer[93].

- En virtud del apartado c) del artículo 139 TRLPI el titular del derecho "sui generis" puede solicitar la retirada y la destrucción de ejemplares ilícitos. La doctrina entiende que con "ejemplar" se refiere a todo soporte en el que se haya almacenado una parte sustancial del contenido de la base de datos protegida[94]. Para que se produzca la destrucción de los ejemplares se requiere que sean ilícitos, es decir, que su extracción o reutilización en forma corporal se haya realizado en contra lo dispuesto por la Ley. Si bien el precepto permite solicitar la retirada o la destrucción, el artículo en su párrafo 2.º establece que el infractor podrá pedir que la destrucción de los ejemplares se efectúe únicamente en la medida necesaria para impedir la explotación ilícita, de acuerdo con el principio de proporcionalidad. Además, en virtud del artículo 139.4 TRLPI, la retirada del comercio y la destrucción de ejemplares no será posible cuando hayan sido adquiridos por terceros de buena fe para uso personal, no obstante será posible la

---

[91] Este es el periodo que el artículo 1962 del Código Civil establece para la prescripción de las acciones reales sobre muebles. BOUZA, M., *El derecho sui ... op. cit.,* pág. 253..

[92] Artículo 140.2 TRLPI.

[93] BOUZA, M., *El derecho sui ... op. cit.,* pág. 254...

[94] Carrasco Perera entiende que ejemplar es todo resultado tangible de una explotación usurpatoria. CARRASCO PERERA, A., en Comentarios, Tecnos, 2ª Ed., pág. 1776.

retirada del comercio a la destrucción cuando se hallen en manos de empresarios[95] que intente comercializarlos o cuando el adquirente no lo fuese de buena fe[96].

Además de las acciones para el cese de la actividad ilícita, ITAINNOVA cuenta con una acción de indemnización que permite que obtenga del infractor una indemnización consistente en el beneficio que hubiera obtenido de no mediar la utilización ilícita, o bien la remuneración que hubiera percibido de haber autorizado la explotación. De esta forma, el perjudicado tiene un derecho de opción que le permite elegir cualquiera de las dos pretensiones, pero una vez que formule judicialmente una de ellas ya no podrá hacer valer la otra, tanto si la demanda se estima, como si se desestima, le vincula como cosa juzgada[97]. La primera pretensión de indemnización consiste en la petición de beneficio presumible, es decir, el lucro cesante o la ganancia que el titular haya dejado de obtener como consecuencia de la infracción[98].

La segunda posibilidad que tiene el perjudicado es la petición de la remuneración que hubiera percibido de haber autorizado la explotación, para ello, se valoraran las condiciones en las que se concedería una licencia contractual en el mercado[99]. Sin embargo, en España no existe ninguna entidad que se dedique a la gestión de los derechos de fabricantes de bases de datos, por lo que no existen tarifas generales que puedan ser utilizadas por los órganos judiciales a la hora de fijar indemnizaciones. Esto implica que la cuestión debe de dejarse en manos de los tribunales los cuales deben apoyarse, sobre todo, en dictámenes periciales[100].

3.6 Limitaciones del derecho "sui generis".

Este derecho "sui generis" no es ilimitado puesto que la DBD estableció ciertas excepciones que han sido traspuestas al derecho español. Concretamente, en el artículo

---

[95] CARRASCO PERERA, A., Comentarios ... *op. cit.,* pág. 1784..

[96] BOUZA, M., *El derecho sui ... op. cit.,* pág. 256...

[97] "Ibídem, pág. 259.

[98] BOUZA, M., *El derecho sui ... op. cit.,* pág. 259. citando a DIEZ PICAZO, L., en Comentarios, Tecnos, pág. 1967.

[99] BOUZA, M., *El derecho sui ... op. cit.,* pág. 260..

[100] BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos… op. cit.,* pág. 198..

135 TRLPI se recogieron tres excepciones y la prohibición de no interpretarlas de forma que causen perjuicio al titular del derecho "sui generis"[101].

Tales excepciones han sido criticadas por muchos expertos y operadores económicos pues consideran que no son suficientes para entornos de *big data*, ni ofrecen un marco jurídico estable para el desarrollo de un buen mercado de bases de datos[102]. A continuación, se realizará un breve análisis de las excepciones más importantes y de su problemática en relación con el *big data.*

El primer límite establecido en el artículo 135.1 TRLPI permite al usuario legitimo la extracción del contenido de bases de datos no electrónicas para fines privados[103]. De esta forma, esta excepción no resulta operativa para el *big data*, debido a que la información contenida se almacena de forma digital en bases electrónicas.

El segundo límite establecido en el artículo 135 TRLPI permite la extracción de información de bases de datos siempre que persiga fines educativos o investigadores. Este límite que perseguía el objetivo de facilitar el desarrollo cultural y educativo de la sociedad, así como promover el desarrollo tecnológico[104], ha sido criticado por la doctrina europea por su difícil interpretación y aplicación en relación con el *big data*[105].

En primer lugar, es una excepción voluntaria que no ha sido incorporada por todos los países europeos. Esto genera una gran incertidumbre jurídica en entornos de *big data* donde la extracción y reutilización de información suele producirse en entornos transnacionales[106].

En segundo lugar, existe incertidumbre en relación con la determinación de las personas que pueden realizar la extracción. Si bien es cierto que la doctrina considera que esta excepción sólo se aplica a usuarios que prueben que actúan guiados por una finalidad docente o investigadora[107], no existe consenso en relación con las figuras que cumplen

---

[101] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1562..

[102] Comisión Europea, Study in support of the evaluation of directive 96/6/EC …op. cit., pág. 14..

[103] PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1563..

[104] BOUZA, M., *El derecho sui … op. cit.,* pág. 228.

[105] RAMOS-SIMÓN, L.F., El uso de las licencias libres en los datos públicos abiertos, Revista española de documentación científica, 2017, Vol. 40, núm. 03. Consejo Superior de Instituciones Científicas. Madrid. http://redc.revistas.csic.es/index.php/redc/article/view/983/1515 [Consulta 01/04/2019].

[106] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 207..

[107] BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos… op. cit.,* pág. 172..

tal condición. Por ejemplo, Bondía considera que «los actos de extracción sólo podrán ser realizados por los profesores e investigadores universitarios, por los doctorandos y por los alumnos de postgrado, pero no por los estudiantes normales, ni por los funcionarios que no están directamente relacionados con la investigación». Por otro lado, tampoco queda claro la situación de los investigadores que actúen en el ámbito de una colaboración pública-privada, ni cual sería, en su caso, la posición de la empresa financiadora[108].

En tercer lugar, esta excepción impide la reutilización de la información lo que afecta de forma directa a la minería de datos, actividad de gran relevancia para la tecnología *machine learning*. Concretamente, la minería de datos permite la simplificación del *big data* para su posterior utilización y análisis por parte de algoritmos. Al prohibir la reutilización se prohíbe, también, la posterior utilización de la información simplificada frustrando el fin de la minería de datos y afectando a la tecnología *machine learning*[109].

Por último, el párrafo final del primer apartado del artículo 135 TRLPI permite las extracciones y/o reutilizaciones para fines de seguridad pública o a efectos de un procedimiento administrativo o judicial[110]. Esta excepción, a diferencia de las anteriores, abarca tanto la extracción como la reutilización.

4. LA DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO SOBRE LOS DERECHOS DE AUTOR EN EL MERCADO ÚNICO DIGITAL.

Parte de la problemática que plantea la legislación europea en relación con tecnologías cómo el *big data* o la minería de datos se ha tratado de resolver en la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se

---

[108] ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos… op. cit.,* pág. 207..

[109] HARGREAVES, GUIBAULS, HANDKE, VALCKRE, MARTENS, "Standardization in the area of innovation and technological development notably in the field of Text and Data Mining: report from the expert group, Luxembourg: Publications Office of the European Union, 2014, pag. 51. Disponible en: https://pure.uva.nl/ws/files/2478182/157208_TDM_report_from_the_expert_group_042014.pdf [Consulta 01/04/2019]

[110]PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley… op. cit.,* pág. 1565...

modifican las Directivas 96/9/CE y 2001/29/CE[111], que fue aprobada por Parlamento Europeo el 26 de marzo de 2019[112], y por el Consejo de la UE el 15 de abril de 2019 (en adelante, DMUD). Es necesario destacar que la Directiva todavía no ha sido traspuesta por ningún Estado miembro debido a que se ha fijado cómo plazo máximo de trasposición el 7 de junio de 2021[114]. Por tanto, hay que tener en cuenta que las siguientes medidas expuestas todavía no son aplicables a la protección del *big data* mediante el derecho "sui generis".

Por lo que interesa al objeto del presente trabajo, uno de los objetivos que persigue la nueva normativa es subsanar la inseguridad jurídica en materia de minería de textos y datos estableciendo una excepción obligatoria para las universidades y otros organismos de investigación respecto del derecho de prohibir la extracción y reutilización de una base de datos. Además, en consonancia con la actual política de investigación de la Unión, que anima a las universidades y los institutos de investigación a colaborar con el sector privado, los organismos de investigación también quedan amparados por la excepción aunque sus actividades de investigación se lleven a cabo en el marco de asociaciones público-privadas (véase cdo. 8.º DMUD).

En primer lugar, la DMUD ha perfilado de forma más concreta el concepto de organismo de investigación. Así pues, *ex* art. 2.1, son organismos de investigación las universidades, los institutos de investigación o cualquiera otras entidades cuyo objetivo sea realizar investigaciones científicas o llevar a cabo actividades educativas que impliquen investigaciones. Además, se exige que la investigación se realice sin ánimo de lucro, conforme a una misión de interés público y de tal manera que una empresa que ejerza una influencia decisiva en dicho organismo no pueda gozar de acceso preferente a los resultados generados por tales investigaciones científicas.

De esta forma, ITAINNOVA, de acuerdo con la DMUD, es un organismo de investigación, debido a que ostenta la condición de instituto público de investigación que realiza investigaciones científicas sin ánimo de lucro y conforme a la misión de

---

[111] Publicado en: «DOUE» núm. 130, de 17 de mayo de 2019, páginas 92 a 124 (18 págs.). Referencia: DOUE-L-2019-130.

[112] Resolución legislativa del Parlamento Europeo, de 26 de marzo de 2019, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital (COM(2016)0593 – C8-0383/2016 – 2016/0280(COD)) (Procedimiento legislativo ordinario: primera lectura).

[114] Art. 29 DMUD.

interés público de fomentar el desarrollo tecnológico de Aragón. Tampoco existe ninguna empresa regional que ejerza mucha influencia sobre ITAINNOVA por su condición de instituto público.

En segundo lugar, la Directiva ha ampliado el conjunto de excepciones previsto en la DBD para el derecho "sui generis" con el objetivo de adaptarlas a la minería de datos, tecnología que posibilita el tratamiento de grandes cantidades de información y que es primordial para la investigación llevada a cabo por universidades, organismos de investigación, instituciones responsables del patrimonio cultural, entre otros (véase cdo. 8.º DMUD).

Dichos organismos o instituciones se enfrentan en la Unión a cierta inseguridad jurídica a la hora de determinar hasta qué punto pueden llevar a cabo actividades de minería de textos y datos de contenidos debido a que, en determinados casos, la minería de textos y datos puede comportar actos protegidos por derechos de autor, por derecho "sui generis" sobre las bases de datos, o por ambos, en particular, la reproducción de obras u otras prestaciones, la extracción de contenidos de una base de datos, o ambos, lo que sucede, por ejemplo, cuando se normalizan los datos en el proceso de minería de textos y datos (véase cdo. 8.º DMUD).

Con el objetivo de resolver toda esta problemática, en la DMUD se prevé que está permitida la extracción y reutilización de partes sustanciales de bases de datos en los siguientes supuestos[115].

- Cuando la extracción y/o reutilización la lleven a cabo organismos de investigación e instituciones responsables del patrimonio cultural con el fin de realizar, con fines de investigación científica, minería de textos y datos de obras u otras prestaciones a las que tengan acceso lícito.

De esta forma, cuando la DMUD sea transpuesta, ITAINNOVA por su condición de organismo de investigación, podrá extraer y reutilizar partes sustanciales de *big data* siempre y cuando tenga como objetivo simplificar la información mediante minería de datos para su posterior uso en otros proyectos.

- Cuando la extracción, reutilización y reproducción se realice de forma legítima para fines de minería de textos y datos.

---

[115] Estas excepciones amplían las ya existentes en la DBD sin llegar a sustituirlas.

- Cuando la extracción, reutilización y reproducción se realice únicamente a efectos de ilustración con fines educativos, en la medida en que ello esté justificado por la finalidad no comercial perseguida, a condición de que dicho uso tenga lugar bajo la responsabilidad de un centro de enseñanza, en sus locales o en otros lugares, o a través de un entorno electrónico seguro al que solo puedan acceder los alumnos o estudiantes y el personal docente del centro; y vaya acompañado de la indicación de la fuente, con inclusión del nombre del autor, salvo que ello resulte imposible.

- Cuando la extracción y/o reutilización se realice con el fin de permitir a las instituciones responsables del patrimonio cultural efectuar copias de las obras u otras prestaciones que se hallen de forma permanente en sus colecciones, en cualquier formato y en cualquier soporte, con la finalidad de conservar tales obras u otras prestaciones y en la medida necesaria para esa conservación.

IV. PROTECCIÓN DEL ALGORITMO EN LA NUEVA LEY DE SECRETOS EMPRESARIALES.

1. INTRODUCCIÓN.

La figura del secreto empresarial lleva existiendo durante muchos años en los diferentes ordenamientos jurídicos europeos a pesar de su escasa regulación. Esto llevó a que, en el año 2016, la UE aprobase la DSE, que tenía como objetivo armonizar la regulación de los secretos empresariales en la UE y establecer un nivel suficiente y comparable de reparación en todo el mercado interior en caso de apropiación indebida de secretos empresariales (véase Preámbulo LSE). Para ello se estableció cómo plazo máximo para su transposición el 9 de junio de 2018. El pasado 21 de febrero de 2019 se publicó en el BOE la LSE, la cual entró en vigor el 13 de marzo de 2019.

Hasta entonces, la escasa regulación de los secretos empresariales se encontraba en el art. 13 LCD, el cual, a pesar de no delimitar el concepto de secreto empresarial[116], tipificaba ciertas violaciones de secretos empresariales como actos de competencia desleal.

[116] La inexistencia de una definición supuso que los tribunales españoles interpretaran el término en el mismo sentido del art. 39.2 de los ADPIC.

Actualmente, dicha regulación ha pasado a ser sustituida por la nueva Ley, de modo que la LCD pasa a remitir a la LSE, disponiendo que «se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales».[117]

Estos cambios legislativos han afectado de forma directa a la protección jurídica de los algoritmos, puesto que la nueva LSE permite protegerlos como secretos empresariales y sustituye la regulación anterior. A continuación, se realizará una síntesis de los aspectos más relevantes de la nueva LSE y de cómo pueden ayudar a proteger el *machine learning.*

2. DEFINICIÓN DE SECRETO EMPRESARIAL.

El art. 1 LSE define el concepto de secreto empresarial de forma muy general, tomando como referente la definición establecida en la Directiva europea y en el ADPIC[118], que venía siendo aplicada por los tribunales españoles[119][120].

Es necesario destacar que nuestro legislador ha decidido modificar la forma en la que la Directiva se refiere a los secretos: en vez de denominarlos "comerciales" ha decidido utilizar el término "empresariales"[121]. Esto se debe a que el término "secreto

---

[117] GARCÍA VIDAL, A., "Diez cuestiones clave sobre la nueva Ley de Secretos Empresariales", 2019. Disponible en: https://www.ga-p.com/wp-content/uploads/2019/02/Analisis-Secretos-empresariales_def.pdf [Consulta 26/03/2019]

[118] Artículo 39 ADPIC

[119] "La nueva Ley de Secretos Empresariales", Clifford Chance, Barcelona, 2019, pág 1. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwitiMDd35_hAhVD1xoKHdFpAogQFjAAegQIAhAC&url=https%3A%2F%2Fonlineservices.cliffordchance.com%2Fonline%2FfreeDownload.action%3Fkey%3DOBWIbFgNhLNomwBl%252B33QzdFhRQAhp8D%252BxrIGReI2crGqLnALtlyZe9HWYWYfTuNQGYVa5WlM4w%252Fp%250D%250A5mt12P8Wnx03DzsaBGwsIB3EVF8XihbSpJa3xHNE7tFeHpEbaeIf%26attachmentsize%3D213077&usg=AOvVaw3WJq2X1N7FHZu9_CsHIvEH [Consulta 26/03/2019]

[120] La definición de secreto empresarial en la nueva LSE es uno de los principales avances en relación con la antigua regulación de la violación de secretos empresariales como actos de competencia desleal recogida en el art.13 LCD. Esto se debe a que en la anterior normativa no se definía el concepto de secreto empresarial lo que llevó a que los tribunales españoles elaborasen sus propias definiciones.

[121] MERCADAL, T., "La nueva Ley de Secretos Empresariales", Bird&Bird, 2019 pág 2. Disponible en: https://www.twobirds.com/~/media/spanish/aprobación-en-españa-de-la-nueva-ley-de-secretos-empresariales.pdf?la=es [Consulta 26/03/2019]

empresarial" comprende tanto el secreto comercial e industrial, la innovación tecnológica, así como la de naturaleza económica, financiera u organizativa[122].

Así pues, de acuerdo con el art. 1 LSE, se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna ciertos requisitos[123]. De esta forma, la LSE ha previsto una definición genérica que permite que los algoritmos sean protegidos por esta figura jurídica siempre y cuando concurran los siguientes requisitos[124]:

- Las secuencias de órdenes que configuran el algoritmo deben de ser secretas en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas (art. 1.1 LSE)[125]. Sin embargo, es necesario tener en cuenta que no se requiere que el algoritmo sea totalmente desconocido ni nuevo. En palabras de Martí y Haro, «la complejidad y el amplio alcance del secreto empresarial explica que no sólo puede ser objeto de este peculiar bien inmaterial una información de utilidad empresarial que nunca ha trascendido a terceros; en ocasiones, lo desconocido y competitivamente útil no son los distintos conocimientos individualmente considerados, sino la peculiar forma en la que éstos se combinan o interactúan, resultado de ello una aplicación no conocida y ventajosa desde el punto de vista desconocido»[126]. De esta forma, los las secuencias de órdenes que conforman el algoritmo pueden ser secreto

---

[122] CNMV, IPN/CNMC/005/18 ANTEPROYECTO DE LEY DE SECRETOS EMPRESARIALES

[123] MERCADAL, T., *"La nueva Ley de Secretos … op. cit.,* pág. 2

[124] Estos requisitos han sido aplicados por la jurisprudencia española desde la regulación de la violación de secretos empresariales como actos de competencia desleal recogida en la LCD. Por ejemplo, la Audiencia Provincial de Barcelona en la Sentencia nº 12269/2005, de julio de 2005, determinó que para que la información empresarial pueda considerarse secreto empresarial es necesario que concurran los siguientes requisitos: 1) que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; 2) que tenga un valor comercial por ser secreta; y 3) que haya sido objeto de medidas razonables, atendidas las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la control. (ECLI: ES:APB:2005:12269) . SAP Madrid de 18 de enero de 2019, núm. 19/2019, ECLI: ES:APM:2019:2366

[125] SAP de Barcelona de 26 de octubre de 2005 aclaró que, para que se cumpla este requisito, basta con un conocimiento o información que no es notorio (AC 2006/365).

[126] STS de 21 de octubre de 2005 (RJ 2005, 8274) y las Sentencias del TJM de Madrid de 9 de diciembre de 2005 (AC 2006,342), y de 13 de Marzo de 2012 (AC 2012, 827).

empresarial aunque sean conocidas por círculos ajenos a aquél en el que son competitivamente útiles o aunque sean conocidas por miembros del círculo en el que es competitivamente útil cuando hayan accedido de forma lícita o por descubrimiento *ex novo*[127].

- Los algoritmos deben de tener un valor comercial por su carácter secreto, pudiendo ser este valor comercial no solo real sino también potencial (véase cdo. 14.º DSE). Para que concurra este requisito, no sólo es necesario que la información tenga valor comercial, sino que también hay que probar su utilidad o ventaja competitiva[128][129]. Los algoritmos son la base creativa de un proyecto de *machine learning* puesto que son los componentes que permiten identificar patrones en el *big data* y hacer predicciones. Su valor depende de su carácter secreto puesto que en el momento en el que pierden su condición secreta cualquier persona con acceso a la información contenida en la base de datos puede obtener las mismas predicciones.
- Por último, los algoritmos deben de haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerlos secretos, tomadas por la persona que legítimamente ejerza su control. La voluntad de mantener secreta la información puede manifestarse de forma tácita (por ejemplo, cuando se adoptan medidas orientadas a garantizar la condición secreta del algoritmo[130]) o expresa (por ejemplo, cuando concurren en el contrato cláusulas de confidencialidad). Según la jurisprudencia[131], el conjunto de medidas adoptadas por el titular de los conocimientos para garantizar su carácter secreto exterioriza el verdadero valor del bien protegido, por lo que su ausencia determina la inexistencia de un

---

[127] MARTÍN ARESTI, P., y DE HARO IZQUIERDO, M., *"Los contratos sobre el Know How"* de Contratos civiles, mercantiles, públicos, laborales e internacionales, con sus implicaciones tributarias, Vol 13, 2014, pág. 396.

[128] STS núm. 6410/2005, de 21 de octubre de 2005 (ECLI: ES:TS:2005:6410) y SSAP Sección 5ª Tarragona de 25 de marzo de 2005 (AC 2008, 977).

[129] MARTÍN ARESTI, P., y DE HARO IZQUIERDO, M., *"Los contratos sobre… op. cit.,* pág. 396.

[130] SAP Barcelona de 26 de noviembre de 2004 (AC 2004/2199) aclaró que la voluntad tácita de conservación del secreto se canaliza a través de medidas de conservación tales cómo vigilancia y control del personal, cámaras de seguridad, encriptado o claves informáticas.

[131] STS de 8 de octubre de 2007 (RJ 2007, 6805) y la SAP de Madrid de 18 de Mayo de 2006 (AC 2006, 1689)

secreto susceptible de protección[132]. ITAINNOVA, en función del proyecto y la información procesada, utiliza diversas herramientas para mantener los algoritmos en secreto. Por un lado, solamente pueden acceder los usuarios autorizados y autentificados mediante el acceso a los servidores a través de puertos asegurados. Además, si la información es de gran relevancia, utilizan herramientas de encriptación. Finalmente, la creación de perfiles usuarios nunca se hace utilizando datos de carácter personal, sino en base a elementos más difíciles de ser suplantados, cómo opiniones.

En conclusión, los algoritmos utilizados en la herramienta Moriarty de ITAINNOVA pueden ser protegidos jurídicamente mediante la figura del secreto empresarial debido a que cumplen los tres requisitos necesarios; ser secretos, tener un valor comercial por su carácter secreto y haber sido objeto de medidas de protección para mantenerlos en secreto.

3. TITULARIDAD, COTITULARIDAD Y LICENCIAS

Tal y como establece el art. 1.2 LSE, el titular de un secreto empresarial es cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo.

ITAINNOVA es un instituto tecnológico con personalidad jurídica propia[133] que ejerce el control sobre el proyecto Moriarty, por lo que es titular de los algoritmos como secreto empresarial.

Además, en el Capítulo III, la Ley prevé la posibilidad de que el secreto pertenezca proindiviso a varias personas, estableciendo un régimen de cotitularidad. En los casos de cotitularidad, la comunidad se regirá por lo acordado por las partes. En defecto de acuerdo, la Ley ha establecido un conjunto de reglas supletorias las cuales permiten que cada titular pueda realizar las siguientes actuaciones de forma independiente al resto de partícipes (art. 5.2 LSE):

a) Explotar el secreto empresarial previa notificación a los demás cotitulares.

b) Realizar los actos necesarios para la conservación del secreto empresarial como tal.

---

[132] MARTÍN ARESTI, P., y DE HARO IZQUIERDO, M., *"Los contratos sobre… op. cit.,* pág. 391.

[133] *Ex* art. 2 del Decreto 88/2015, de 5 de mayo, del Gobierno de Aragón, por el que se aprueban los Estatutos del Instituto Tecnológico de Aragón.

c) Ejercitar las acciones civiles y criminales en defensa del secreto empresarial siempre y cuando lo notifique al resto de partícipes para que estos decidan sí unirse o no a la mismas[134].

A todo lo anterior se suma la regulación, por primera vez en nuestro ordenamiento y sin que ello fuera exigido por la DSE, de los secretos empresariales como objeto de derecho de propiedad (Capítulo III LSE)[135]. De esta forma, se atribuye a su titular o titulares un derecho subjetivo de naturaleza patrimonial susceptible de ser objeto de transmisión, en particular, de cesión o transmisión a título definitivo y de licencia o autorización de explotación con el alcance objetivo, material, territorial y temporal que en cada caso se pacte (véase Preámbulo III LSE). Esto es especialmente relevante para el *machine learning* puesto que la mayoría de los proyectos de inteligencia artificial son llevados a cabo por empresas que compiten en el mercado, de esta forma se permite que el algoritmo como secreto empresarial pueda ser trasmitido a otras empresas en función de las necesidades de las primeras.

En relación con el régimen general de licencia de secretos empresariales[136], el art. 6.1 LSE establece que las partes podrán pactar el alcance objetivo, material, territorial y temporal de las licencias. En caso de que las partes no pacten nada al respecto, se establece un régimen supletorio en el art. 6.2 LSE. Concretamente, la LSE considera que existen dos tipos de licencias: la exclusiva y la no exclusiva. La primera de ellas impide al licenciante el otorgamiento de otras licencias y también, la utilización de la misma a excepción de que en el contrato se contemple expresamente esa opción. Por el contrario, la licencia no exclusiva[137] permite al licenciante el otorgamiento de nuevas licencias y la libre utilización del secreto empresarial.

Por último, se preceptúa que, salvo que se pacte expresamente, el licenciatario no podrá ceder el contrato a terceros ni conceder sublicencias y que el licenciatario o

---

[134] Esta regulación constituye un complemento de nuestro legislador respecto de la Directiva, que no trata estas cuestiones.

[135] URÍA MENÉNDEZ, "Ley 1/2019, de 20 de Febrero, de Secretos Empresariales", 2019, pág 7. Disponible en: https://www.uria.com/documentos/circulares/1060/documento/8453/Ley_Secretos_Empresariales.pdf [Consulta 26/03/2019]

[136] La regulación de la licencia de secretos empresariales es similar a la establecida en la LP.

[137] Se presume que la licencia es no exclusiva.

sublicenciatario estará obligado a adoptar las medidas necesarias para evitar la violación del secreto empresarial[138].

4. OBTENCIÓN, UTILIZACIÓN O REVELACIÓN ILÍCITAS DE SECRETOS EMPRESARIALES

En el art. 3 LSE se prevén tres conductas que pueden constituir por sí mismas violación de secreto empresarial[139]. A continuación, se realizará un análisis de los aspectos más importantes de dichas conductas en relación con la violación de un algoritmo cómo secreto empresarial.

4.1 La obtención del secreto empresarial.

Conducta consistente en apoderarse de la información o de la fuente, de la que se obtiene la misma, calificada como secreto empresarial[140]. En relación con el *machine learning*, esta conducta consistiría en apoderarse de las secuencias de órdenes que componen el algoritmo.

Para que esta actividad sea ilícita es necesario, además, que se produzca mediante el acceso, apropiación o copia no autorizada de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes, que contengan el secreto empresarial o a partir de los cuales se pueda deducir[141], o que se realice mediante una actividad contraria a las prácticas comerciales leales (art. 3.1 LSE).

En el caso de los algoritmos lo más común es que el acceso, apropiación o copia no autorizada se produzca sobre documentos o ficheros electrónicos debido a que las series de órdenes que componen el algoritmo se suelen escribir en lenguaje de

---

[138] GARCÍA VIDAL, A., "Diez cuestiones clave sobre … *op. cit*.

[139] La delimitación de las conductas ilícitas por parte de la LSE ha supuesto un gran cambio en relación con la normativa anterior que únicamente reconocía cómo actos de violación de secretos empresariales la divulgación, explotación y adquisición de información secreta.

[140] URÍA MENÉNDEZ, "*Ley 1/2019, de 20 de Febrero, de Secretos… op. cit.,* pág. 5.

[141] La LSE ha recogido la opinión mayoritaria de la doctrina que considera que la obtención de la información secreta se puede realizar de múltiples formas tales como copiándola, memorizándola, apropiándose de los soportes materiales que la contienen, entre otras. SUÑOL LUCEA, A., *El secreto empresarial. Un estudio del artículo 13 de la Ley de Competencia desleal*, Thomson Reuters, Cizur Menor, 2009.

programación[142].

4.2. La utilización del secreto empresarial.

La utilización del secreto empresarial es la actividad consistente en emplear de cualquier forma la información calificada como secreto empresarial[143]. Este es el mayor riesgo al que se enfrentan los creadores de *machine learning* debido a que la utilización ilícita del algoritmo por parte de competidores les permite obtener predicciones, las cuales son el verdadero valor del proyecto de *machine learning*.

4.3. La revelación del secreto empresarial.

Por otro lado, la revelación del secreto empresarial es la actividad consistente en comunicar la información al público o sólo a algunos terceros[144].

Para que la utilización y/o revelación del secreto empresarial sean ilícitas se exige la previa obtención ilícita o la vulneración de un pacto u obligación de confidencialidad o de cualquier otra obligación de no revelar el secreto empresarial o el incumplimiento de una obligación contractual o de cualquier otra índole que limite la utilización del secreto empresarial (art. 3.2 LSE).

Esto adquiere gran relevancia en el ámbito laboral de ITAINNOVA, puesto que trabajadores involucrados en el proyecto de *machine learning* y familiarizados con los algoritmos utilizados se pueden ver tentados a revelar su contenido a competidores. Al respecto, la Audiencia Provincial de Barcelona en Sentencia núm. 12269/2005, de 13 de julio, hace una interesante reflexión al determinar que hay que distinguir entre secreto empresarial y las informaciones que formen parte de las habilidades, capacidades y experiencia de carácter general de un trabajador adquiridas a lo largo de su carrera profesional[145]. Este límite vendría representado por aquellos conocimientos o información, titularidad de hecho del empresario, que constituyen secreto empresarial, al cual se ha tenido acceso legítimamente en tanto se mantenía su relación con la anterior empresa, pero con deber de reserva.

---

[142] MUELLER, J., y MASSARON, L., *"Machine Learning for dummies",* John Wiley & Sons Inc, 2016.

[143] URÍA MENÉNDEZ, "*Ley 1/2019, de 20 de Febrero, de Secretos… op. cit.,* pág. 5.

[144] "Idem".

[145] ECLI: ES:APB:2005:12269

De esta forma, la utilización de la habilidad que poseen los trabajadores de ITAINNOVA para el desarrollo de algoritmos nunca puede constituir una revelación de secreto empresarial. Por el contrario, la revelación de la serie de instrucciones en lenguaje matemático que componen los algoritmos a los que han tenido acceso mientras duraba su relación laboral con ITAINNOVA sí que es una actividad ilícita. Por último, en el art. 1.3 LSE se establece que la obtención, utilización o revelación de un secreto empresarial se consideran asimismo ilícitas cuando la persona que las realice, en el momento de hacerlo, sepa o, en las circunstancias del caso, debiera haber sabido que obtenía el secreto empresarial directa o indirectamente de quien lo utilizaba o revelaba de forma ilícita.

5. ACCIONES DE DEFENSA DE SECRETOS EMPRESARIALES.

Frente a los actos de violación de secretos empresariales recogidos en el apartado anterior, y sin perjuicio de la aplicación de los artículos 278 y 279 del Código Penal[146] para los casos más graves, la Ley prevé un conjunto de acciones civiles muy similares a las recogidas en la LCD que los titulares de algoritmos protegidos cómo secretos empresariales pueden ejercitar[147].

En concreto, las acciones civiles protectoras de los secretos empresariales ejercitables son las tendentes a la declaración de la violación del secreto empresarial, la cesación y/o prohibición de los actos de violación del secreto empresarial, la prohibición de fabricar, ofrecer, comercializar o utilizar las mercancías infractoras, así como su importación, exportación o almacenamiento para tales fines, la aprehensión de las mercancías infractoras, la remoción, consistente en que se proceda a entregar al demandante total o parcialmente los documentos, objetos, materiales, etc., en que se contenga el secreto empresarial, así como su destrucción parcial o total, la indemnización de daños y perjuicios irrogados, siempre y cuando haya mediado dolo o culpa del infractor y la publicación o difusión completa o parcial de la sentencia (art. 9.1 LSE).

---

[146] Publicado en: «BOE» núm 281, de 24-11-1995. Referencia: BOE-A-1995-25444.

[147] GARRIDO ABOGADOS, "Nota informativa - Ley 1/2019, de 20 de febrero, de Secretos Empresariales que transpone la Directiva Europea 2016/943", 2019, pág. 2. Disponible en: https://garrido.es/wp-content/uploads/2019/02/Nota-informativa.-Ley-de-secretos-empresariales.pdf [Consulta 26/03/2019]

Sin embargo, para la protección de los algoritmos como secreto empresarial, son especialmente relevantes la cesación y/o prohibición de los actos de violación de secretos empresariales, pues de esta forma se evita que los infractores sigan utilizando los algoritmos, y las acciones de remoción que permiten la destrucción de los documentos en poder del infractor. Mediante estas dos acciones, se puede proteger la inversión que el titular del algoritmo protegido cómo secreto empresarial ha realizado en un proyecto de *machine learning* debido a que se evita que el infractor pueda seguir utilizando el algoritmo para obtener predicciones.

Las medidas acordadas en virtud del ejercicio de las anteriores acciones deberán atender a los parámetros de proporcionalidad y a las circunstancias del caso, tales como las características del secreto empresarial vulnerado, sus consecuencias, el comportamiento del infractor, etc[148].

También, es necesario destacar la posibilidad de ejercitar las acciones civiles anteriormente mencionadas frente a terceros adquirentes de buena fe, entendiéndose por tales, quienes en el momento de la utilización o de la revelación no sabían o, en las circunstancias del caso, no hubieran debido saber que habían obtenido el secreto empresarial directa o indirectamente de un infractor (art. 8 LSE). En estos casos no cabrá la acción de indemnización de daños y perjuicios, que solo se prevé en casos en que haya intervenido dolo o culpa del infractor (art. 9.1.g LSE).

Sin embargo, la Ley ha previsto la posibilidad de que, a petición de la parte demandada, tales medidas puedan ser sustituidas por el pago a favor de la parte demandante de una indemnización pecuniaria, siempre que ésta resulte razonablemente satisfactoria y que la ejecución de tales medidas fuera a causar al demandado un perjuicio desproporcionado. Dicha indemnización no excederá del importe que hubiera tenido que pagar el demandado por la concesión de una licencia que habría permitido utilizar el algoritmo durante el período en el que se produjo la violación del secreto empresarial (art. 9.7 LSE). Sin embargo, esta medida alternativa plantea problemas en relación con la violación de algoritmos protegidos cómo secretos empresariales debido a la inexistencia, actualmente, de un mercado de licencias y a la dificultad de determinar la cantidad que habría que pagar por ella.

---

[148] GARRIDO ABOGADOS, "Nota informativa - Ley 1/2019, de 20 de febrero, de Secretos Empresariales … *op. cit.,* pág. 3..

6. OBTENCIÓN, UTILIZACIÓN O REVELACIÓN LÍCITAS DE SECRETOS EMPRESARIALES.

El titular de un algoritmo protegido cómo secreto empresarial puede ejercitar diversas acciones civiles contra actos de violación del secreto empresarial consistentes en la obtención, utilización o revelación ilícita del secreto empresarial. Sin embargo, el legislador, por primera vez, ha regulado en la LSE una serie de supuestos en los que la obtención, utilización o revelación de secretos empresariales son lícitos y, por tanto, frente a los que el titular del secreto empresarial no puede ejercitar ninguna acción.

En primer lugar, existen ciertos medios de obtención de la información protegida cómo secreto empresarial que son lícitos. En el art. 2.1 LSE se recogen los siguientes:

a) El descubrimiento o la creación independientes. Este medio afecta especialmente a la protección del algoritmo como secreto empresarial debido a que no se estará violando el secreto empresarial en los casos en los que, mediante investigaciones independientes, se llegue a desarrollar el mismo o un similar algoritmo.

b) La ingeniería inversa consistente en la observación, estudio, desmontaje o ensayo de un producto u objeto que se haya puesto a disposición del público. Este medio de obtención del secreto empresarial es probable que ocurra en relación con los algoritmos utilizados en la herramienta Moriarty. Esto se debe a que Moriarty es un programa informático utilizado por empresas, las cuales pueden, mediante ingeniería inversa, tratar de conocer el algoritmo utilizado en el programa.

c) El ejercicio del derecho de los trabajadores y los representantes de los trabajadores a ser informados y consultados, de conformidad con el Derecho europeo o español y las prácticas vigentes;

d) Cualquier otra actuación que, según las circunstancias del caso, resulte conforme con las prácticas comerciales leales, incluidas la transferencia o cesión y la licencia contractual del secreto empresarial, de acuerdo con el Capítulo III.

Por otro lado, se prevén ciertas circunstancias en las cuales la obtención, utilización o revelación de un secreto empresarial son lícitas. Así pues, la obtención, utilización y revelación de secretos empresariales se reputará lícita cuando i) se lleve a efecto en el ejercicio de los derechos fundamentales de expresión e información; ii) con la finalidad

de descubrir actividades irregulares vinculadas a dicho secreto empresarial; iii) cuando los trabajadores lo hayan puesto en conocimiento de sus representantes legales de ser ello necesario para el ejercicio de funciones que éstos tengan legalmente atribuidas y, por último, iv) con el fin de proteger un interés legítimo reconocido por el Derecho europeo o español (art. 2.3 LSE).

V. CONCLUSIONES

Dentro de la llamada cuarta revolución industrial, la inteligencia artificial ocupa un papel protagonista. Concretamente, el *machine learning* se está posicionando como uno de los sectores más punteros debido a su gran aplicabilidad práctica. A nivel regional, ITAINNOVA es una de las pocas entidades que está apostando por el desarrollo de esta tecnología debido a la gran inversión de recursos que supone desarrollar este tipo de tecnología.

La principal problemática jurídica que plantea el desarrollo de este tipo de proyectos es que, actualmente, no existe una figura jurídica que proteja las soluciones de *machine learning* en su conjunto; sino que existen diversas normativas que, por un lado, protegen los algoritmos y, por otro lado, el *big data*.

En relación con el *big data*, actualmente no existe una normativa que se adapte plenamente a esta nueva tecnología. En lo relativo a derechos de autor, ITAINNOVA no ha dispuesto de forma original el contenido del *big data* utilizado, por lo que no puede ser protegido como base de datos.

Por otro lado, el TRLPI, al regular el derecho "sui generis" sobre las bases de datos, adopta una definición de base de datos muy escueta en comparación con el *big data.* Concretamente, no tiene en cuenta que los datos utilizados por el *big data* son masivos, desestructurados y se actualizan constantemente. A pesar de lo anterior, el derecho "sui generis" sobre las bases de datos es la figura jurídica que, actualmente, mejor protege jurídicamente el *big data* utilizado en las soluciones de *machine learning*. De esta forma, cómo se ha estudiado a lo largo del trabajo, la inversión sustancial realizada por ITAINNOVA para la obtención, presentación y verificación del contenido del *big data* utilizado en el proyecto Moriarty cumple los requisitos para ser protegida mediante el derecho "sui generis", lo que permite a ITAINNOVA prohibir la extracción y/o

reutilización de la totalidad o de una parte sustancial del *big data* de cada una de las versiones que se generen cada 31 de diciembre durante 15 años.

En relación con los algoritmos, hasta la entrada en vigor de la LSE no existía una figura jurídica específica que regulase su protección, lo cual generaba una gran inseguridad jurídica. Concretamente, el art. 13 LCD regulaba las violaciones de secretos empresariales cómo actos de competencia desleal sin delimitar los requisitos necesarios para que una información fuese catalogada cómo secreto empresarial. Toda esta problemática ha sido solucionada con la entrada en vigor de la LSE.

Así pues, la nueva LSE permite proteger la secuencia de instrucciones que forman los algoritmos cómo secreto empresarial siempre que sean secretas, que tengan un valor comercial por su carácter secreto y que hayan sido objeto de medidas para mantenerlas en secreto. Cómo se ha expuesto, ITAINNOVA cumple todos los requisitos necesarios para poder proteger los algoritmos utilizados en el proyecto Moriarty como secreto empresarial, lo que le permite ejercer acciones contra aquellos que obtengan, utilicen o revelen ilícitamente los algoritmos utilizados en el proyecto. A pesar de lo anterior, ITAINNOVA no podrá impedir que competidores lleguen a desarrollar algoritmos similares mediante diversas fórmulas como ingeniería inversa o creación independiente.

Para terminar, es necesario destacar que actualmente la tecnología está avanzando rápidamente lo que dificulta que el legislador se adapte de forma efectiva a estos cambios. En relación con el tema tratado, es previsible que en los próximos años el legislador europeo modifique la normativa de forma que se adapte plenamente al concepto de *big data* y *machine learning.*

BIBLIOGRAFÍA

TRABAJOS DOCTRINALES

AZUAJE PIRELLA, M., y FINOL GONZÁLEZ, D., Big Data, algoritmos y propiedad intelectual, Revista Anuario de Propiedad Intelectual, Nº 2016, 2017.

BATALLER I RUIZ, E., *El derecho sui generis sobre base de datos: génesis, evolución y perspectivas,* Aranzadi-Thomson Reuters, Cizur Menor, 2009.

BERCOVITZ RODRIGUEZ CANO, R., Comentarios a la Ley de Propiedad Intelectual, Editorial Tecnos SA, Madrid, 1997.

BONDÍA ROMÁN, F., *"Comentarios a la Ley de Propiedad Intelectual"*, Editorial Civitas, Madrid, 1997, pág. 189.

BOVENBERG, J.A. Should Genomocs Companies set up Data Base in Europe?. The EU Database protection Directive Revisited, EIPR, vol 23, nº8, agosto de 2001, pág. 365.

BOUZA LÓPEZ, M.A., *"El Derecho Sui Generis del fabricante de Bases de Datos"*, Editorial Reus, SA, Madrid, 2001.

CARBAJO CASCÓN, F., "*Reproducción y copia privada en el entorno digital",* RDNT, 2003, núm 2, pág. 56.

CARRASCO PERERA, A., Comentario al artículo 7, en *"Comentarios a la Ley de Propiedad Intelectual"*, Editorial Tecnos SA, Madrid, 1997.

COLLE, M, *"Algoritmos, grandes datos e inteligencia artificial en la red. Una visión crítica".* Colección mundo digital. 2017.

COMISIÓN EUROPEA, Study in support of the evaluation of directive 96/6/EC on the legal protection of databases", 2018, Directorado-General de Redes de Comunicaciones, Contenido y Tecnología. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1/language-en/format-PDF/source-92832355 [Consulta 01/04/2019] Pág. 31-32.

COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA. *"IPN/CNMC/005/18 Anteproyecto de Ley de Secretos Empresariales*". 15 de marzo de 2018.

FERNÁNDEZ, M, *La protección de la Inteligencia Artificial determina el desarrollo tecnológico,* Bird&Bird, 2019. Disponible en: http://www.legaltoday.com/actualidad/noticias/la-proteccion-de-la-inteligencia-artificial-determina-el-desarrollo-tecnologico [Consulta 14/05/2019].

GARCIA DEL POLLO, R., y GARCÍA, S., Implicaciones legales del machine learning, Revista Actualidad Mercantil, Tirant Lo Blanch, 2019, pág. 459.

HARGREAVES, GUIBAULS, HANDKE, VALCKRE, MARTENS, "Standardization in the area of innovation and technological development notably in the field of Text and Data Mining: report from the expert group, Luxembourg: Publications Office of the European Union, 2014, pág. 51. Disponible en: https://pure.uva.nl/ws/files/2478182/157208_TDM_report_from_the_expert_group_042014.pdf [Consulta 01/04/2019]

KURZWEIL, R., *The Age of Intelligent Machines,* The MIT press Cambridge, MA, USA, 1990.

MARTÍN ARESTI, P., y DE HARO IZQUIERDO, M., *"Los contratos sobre el Know How"* de Contratos civiles, mercantiles, públicos, laborales e internacionales, con sus implicaciones tributarias, Vol 13, 2014, pág. 397.

MARTIN VILLAREJO, A., Comentario al artículo 167*,* en " *Comentarios a la Ley de Propiedad Intelectual",* Editorial Aranzadi, SA, Cizur Menor (Navarra), 2007.

MAYER-SCHÖNBERGER, V., Big data. La revolución de los datos masivos, (Antonio Iriarte, trad.), Turnes Publicaciones, Madrid, 2013, pág. 639.

MUELLER, J., y MASSARON, L., *"Machine Learning for dummies",* John Wiley & Sons Inc , 2016.

PALAU RAMÍREZ, F. y PALAO MORENO, G., *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017.

PÉREZ SANZ, C. "Aspectos legales del Big Data". Revista índice. 2016. Disponible en: http://www.revistaindice.com/numero68/p18.pdf

PÉREZ DE ONTIVEROS BAQUERO, C., En relación con el derecho de autor en *"Comentarios a la Ley de Propiedad Intelectual"*, Editorial Tecnos SA, 2ª Ed.,Madrid, 1997, pág. 598 .

RAMOS-SIMÓN, L.F., El uso de las licencias libres en los datos públicos abiertos, Revista española de documentación científica, 2017, Vol. 40, núm. 03. Consejo Superior de Instituciones Científicas. Madrid. http://redc.revistas.csic.es/index.php/redc/article/view/983/1515 [Consulta 01/04/2019].

RICH, E y KNIGHT, K., *Artificial Intelligence,* McGraw Hill, 1991, pág. 3.

ROMEU I CÓNSUL, R., *Capítulo VII: Las nuevas bases de datos. Big data, desestructuración e inteligencia artificial* de Nuevos desafíos para el Derecho de Autor: robótica, inteligencia artificial, tecnología, director: NAVAS NAVARRO, S., Reus Editorial, Madrid, 2019.

SAIZ GARCÍA, C., Las obras creadas por sistemas de inteligencia artificial y su protección por el derecho de autor, Revista para el análisis del Derecho INDRET, Nº1, 2019, Barcelona. Disponible en: http://www.indret.com/pdf/1446.pdf [Consulta 28/03/2019].

SCHWAAB, K., *La cuarta revolución industrial,* Debate, World Economic Forum, Madrid, 2016, pág. 12-17.

SUÑOL LUCEA, A., *El secreto empresarial. Un estudio del artículo 13 de la Ley de Competencia desleal,* Thomson Reuters, Cizur Menor, 2009.

VIVAS TESÓN, I. *"La tutela sui generis de las bases de datos" ,* Revista de Derecho Patrimonial, 2008, Núm. 21, pág. 159-174, Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjo7Pqgk6XgAhWSlhQKHVDmDlsQFjAAegQIBhAC&url=https%3A%2F%2Fidus.us.es%2Fxmlui%2Fbitstream%2Fhandle%2F11441%2F60201%2FLa%2520tutela%2520sui%2520generis....PDF%3Fsequence%3D1&usg=AOvVaw3B-UvGq9yM56JWUu71h970 [Consulta: 05/02/2019]

REFERENCIAS

Instituto Tecnológico de Aragón, 2018, Disponible en: https://itainnova.es/es/itainnova [Consulta 26/03/2019]

Machine learning: inteligencia artificial que esta cambiando el mundo. Artículo publicado por Unidad de Inteligencia de Negocios 2019 Disponible:

http://mim.promexico.gob.mx/work/models/mim/templates-new/Publicaciones/Notas/Machine-Learning.pdf [Consulta: 14/02/2019]

¿Qué es Machine Learning y cómo se usa en Big Data? Artículo de Universia España 12/09/2017. Disponible en: http://noticias.universia.es/ciencia-tecnologia/noticia/2017/09/12/1155659/machine-learning-como-usa-big-data.html [Consulta: 25/02/2019]

¿Qué es Machine Learning?, Artículo de Instituto Internacional Español de Marketing Digital (IIEMD). Disponible en: https://iiemd.com/machine-learning/que-es-machine-learning [Consulta: 25/02/2019]

Algoritmo o software: ¿dónde reside mi propiedad intelectual?. Artículo de ECIJA 16/11/2016. Disponible en: https://ecija.com/algoritmo-software-donde-reside-propiedad-intelectual/ [Consulta: 25/02/2019]

Diez cuestiones claves sobre la nueva Ley de Secretos Empresariales, Artículo de Angel García Vidal en Gómez-Acebo & Pombo, Febrero 2019. Disponible en: https://www.ga-p.com/wp-content/uploads/2019/02/Analisis-Secretos-empresariales_def.pdf [Consulta: 20/03/2019]

"La nueva Ley de Secretos Empresariales", Clifford Chance, Barcelona, 2019, pág 1. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwitiMDd35_hAhVD1xoKHdFpAogQFjAAegQIAhAC&url=https%3A%2F%2Fonlineservices.cliffordchance.com%2Fonline%2FfreeDownload.action%3Fkey%3DOBWIbFgNhLNomwBl%252B33QzdFhRQAhp8D%252BxrIGReI2crGqLnALtlyZe9HWYWYfTuNQGYVa5WlM4w%252Fp%250D%250A5mt12P8Wnx03DzsaBGwsIB3EVF8XihbSpJa3xHNE7tFeHpEbaeIf%26attachmentsize%3D213077&usg=AOvVaw3WJq2X1N7FHZu9_CsHIvEH [Consulta 26/03/2019]

MERCADAL, T., "La nueva Ley de Secretos Empresariales", Bird&Bird, 2019 pág 2. Disponible en: https://www.twobirds.com/~/media/spanish/aprobación-en-españa-de-la-nueva-ley-de-secretos-empresariales.pdf?la=es [Consulta 26/03/2019]

URÍA MENÉNDEZ, "Ley 1/2019, de 20 de Febrero, de Secretos Empresariales", 2019, pág 7. Disponible en: https://www.uria.com/documentos/circulares/1060/documento/8453/Ley_Secretos_Empresariales.pdf [Consulta 26/03/2019]

GARRIDO ABOGADOS, "Nota informativa - Ley 1/2019, de 20 de febrero, de Secretos Empresariales que transpone la Directiva Europea 2016/943", 2019, pág. 2. Disponible en: https://garrido.es/wp-content/uploads/2019/02/Nota-informativa.-Ley-de-secretos-empresariales.pdf [Consulta 26/03/2019]

LEGISLACIÓN

Ley 3/1991, de 10 de enero, de Competencia Desleal. (Publicado en: «BOE» núm. 10, de 11/01/1991. Referencia: BOE-A-1991-628).

Directiva 2016/943 del Parlamento europeo y del Consejo de 8 de 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. (Publicado en: Diario Oficial núm. L 157 de 15/06/2016 pp.1-18)

Ley 1/2019, de 20 de febrero, de Secretos Empresariales. (Publicado en: «BOE» núm. 45 de 21/02/2019. Referencia: BOE-A-2019-2364)

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. (Publicado en: «BOE» núm. 97 de 22/04/1996. Referencia: BOE-A-1996-8930)

Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. (Publicado en: Diario Oficial núm. OJ L 77, 27.3.1996, p. 20-28).

JURISPRUDENCIA

Sentencia de la Audiencia Provincial de Barcelona núm. 443/2005 de 26 de octubre de 2005 (ECLI: ES:APB:2005:12412)

Sentencia de la Audiencia Provincial de Barcelona núm. 12269/2005, de 13 de julio de 2005 (ECLI: ES:APB:2005:12269).

Sentencia de la Audiencia Provincial de Madrid núm. 19/2019, de 18 de enero de 2019 (ECLI: ES:APM:2019:2366)

Sentencia de la Audiencia Provincial de Madrid de 18 de Mayo de 2006 (AC 2006, 1689)

Sentencia del TJUE de 2 de mayo de 2012, caso SAS Institute Inc contra World Programming (ECLI:EU:C:2012:259).

Sentencia del TJCE de 3 de julio de 2012, caso UsedSoft GmbH vs Oracle Internacional Corp (ECLI:EU:C:2012:407).

Sentencia del TJUE de 5 marzo 2009, asunto C-547/07, caso Apis-Hristovich EOOD contra Lakord (ECLI:EU:C:2009:132).

Sentencia del TJUE de 1 de marzo de 2012, asunto C-604/10, caso Football Dataco Ltd y otros v. Yahoo UK Ltd. y otros (ECLI: ES:TS:2012:9153).

Sentencia del TJUE de 9 de noviembre de 2004, caso C-444/02, asunto Fixtures Marketing (ECLI:EU:C:2004:697).

Sentencia del Tribunal Supremo núm. 6410/2005, de 21 de octubre de 2005 (ECLI: ES:TS:2005:6410)