ADI 41 (2020-2021): 193-218

LA PROTECCIÓN DE LOS DATOS COMO SECRETO EMPRESARIAL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

THE PROTECTION OF DATA AS A TRADE SECRET IN THE AGE OF ARTIFICIAL INTELLIGENCE

ÁUREA SUÑOL*

RESUMEN

Este trabajo examina la protección de los datos como secreto empresarial en el marco de la inteligencia artificial y defiende que aquella logra alcanzar un equilibro razonable entre incentivar su recopilación y creación y permitir su acceso y uso por terceros.

Palabras clave: secretos empresariales, datos, inteligencia artificial, aprendizaje automático, datos de entrenamiento.

ABSTRACT

This paper analyse the protection of data as a trade secret in the context of artificial intelligence and argues that it strikes a reasonable balance between providing incentives for data collection and generation and allowing third parties to access and use the data.

Keywords: trade secrets law, datasets, artificial intelligence, learning-machine, training data.

* Profesora Agregada Interina de la Universidad Pompeu Fabra. Dirección de correo electrónico: *aurea.sunol@upf.edu*. Agradezco las valiosas observaciones realizadas por los revisores anónimos.

Fecha de recepción: 7 de abril de 2021 // Fecha de aceptación: 8 de mayo de 2021

I. INTRODUCCIÓN

El futuro de la innovación depende en gran medida de la inteligencia artificial (en adelante, «IA») y de otras tecnologías emergentes tales como la robótica avanzada y la computación cuántica. Como señala el Libro Blanco sobre Inteligencia Artificial, esta se asienta sobre dos pilares esenciales: datos y algoritmos[1]. Así sucede especialmente en el aprendizaje automático, el sub-campo de IA más exitoso, que consiste en la identificación de patrones en los datos disponibles y en la aplicación subsiguiente del conocimiento adquirido a nuevos datos[2] y que se usa en un amplio abanico de aplicaciones comerciales y de investigación (*ad ex*. enseñar a los automóviles a conducir de forma autónoma, a reconocer objetos en una imagen, etc.). Gracias a los datos, los agentes pueden desarrollar algoritmos complejos que hacen posible que ordenadores simulen o reproduzcan habilidades cognitivas similares a las de los seres humanos. La recopilación y tratamiento de datos permiten obtener más datos, los cuales sirven, a su vez, para mejorar el funcionamiento de los algoritmos. En palabras de Balkin, parafraseando a Kant, «*algorithms without data are empty; data without algorithms are blind*[3].

Existe cierto consenso en reconocer que la recopilación y generación de datos en el contexto digital requiere, en ocasiones y determinados sectores, una inversión significativa. Parece, pues, necesario estimular a los operadores a invertir en su creación. Los derechos de propiedad intelectual en sentido amplio se orientan, en su mayoría, justamente a ese fin. Sin embargo, conceder una exclusiva sobre los datos tiene su lado oscuro: veta o limita su acceso y uso por terceros, justo el efecto contrario al perseguido por la política estratégica de la Comisión Europea sobre economía de los datos, como muestra, entre otros textos, la reciente Propuesta de Reglamento de gobernanza de datos[4]. No es de extrañar, por ello, que el Parlamento Europeo ha advertido en su resolución sobre

[1] *Vid*. Libro Blanco sobre la inteligencia artificial —un enfoque europeo orientado a la excelencia y la confianza—, 19 de febrero de 2020 [COM (2020) 65 final], pág. 20.

[2] *Vid*. Comisión Europea, Inteligencia Artificial para Europa, COM (2018) 237 final, pág. 11.

[3] *Vid*. BALKIN (2017), pág. 1220.

[4] Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de datos), Bruselas, 25 de noviembre de 2020 COM (2020)767 final.

una eventual regulación en el ámbito de las tecnologías de IA que es necesario evaluar si las normas sobre propiedad intelectual constituyen una herramienta adecuada para proteger los datos[5].

En este trabajo mostraremos que el sistema de protección jurídica del secreto empresarial establecido en la Ley 1/2019, de 20 de febrero, de *Secretos Empresariales* (en adelante «LSE»), que traspone a nuestro ordenamiento la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio, *relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos empresariales) contra su obtención, utilización y revelación ilícitas* (en adelante, «La Directiva») logra alcanzar un equilibrio razonable entre ambos propósitos: incentivar la recopilación y creación de datos (*vid*. *infra* 3) y permitir que terceros accedan a ellos y los utilicen (*vid*. *infra* 4). Por ello es a nuestro juicio y parafraseando a W. Churchill «el peor sistema de protección de los datos, a excepción de todos los demás que se han inventado». Convendrá, con todo, examinar primero los requisitos que deben reunir los datos para merecer la condición de secreto empresarial (*vid*. *infra* 2).

II. LOS DATOS COMO SECRETO EMPRESARIAL

La Directiva ha regulado el concepto de secreto empresarial. El objeto susceptible der ser protegido como tal y los requisitos que este debe reunir al efecto quedan, pues, fijados en ella —y solo en ella—[6]. Los Estados miembros no tienen margen de maniobra al respecto[7]. Por ello, la LES ha recogido en esencia esa noción en su artículo 1.1 aunque, como veremos, se ha desviado en algún extremo.

En particular, según el artículo 2.1 del Directiva, el objeto susceptible de constituir un secreto empresarial es cualquier información que reúna los siguientes requisitos: a) *ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas;* b) *tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto,* c) *haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control*.

---

[5] *Vid*. considerando 18.º de la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial [2020/2015(INI)].

[6] Huelga decir, por tanto, que las condiciones que el Reglamento (UE) núm. 316/2014, relativo a la aplicación del artículo 101.3 del Tratado de Funcionamiento de la Unión Europea a determinadas categorías de acuerdos de transferencia de tecnología, exige para calificar a un conjunto de informaciones de «conocimientos técnicos» a los efectos de ese texto para nada determinan los requisitos que deben concurrir en una información para constituir un secreto empresarial. De hecho, esas condiciones, salvo, si acaso, en la referencia al término «secreta», en nada se parecen a los requisitos establecidos en la Directiva. Y es lógico que así sea, pues el contexto en el que se enmarcan y la finalidad que se persigue al exigirlas (esto es: que el acuerdo que articula su transferencia se beneficie de la exención automática de la normativa de competencia al amparo del art. 101.3 TFUE) no guarda relación con el marco y objetivo al que se orienta la protección de los secretos empresariales. *Vid*., al respecto, Suñol (2009), págs. 144 y 145 e ídem (2020), págs. 9 y 10.

[7] *Vid*. considerando 14 de la Directiva, que advierte de la necesidad de formular un concepto homogéneo de secreto empresarial.

Como es de ver, la Directiva (y, por ende, la LSE) recoge de forma casi idéntica el concepto de secreto empresarial establecido en el artículo 39.2 del acuerdo sobre los ADPIC[8]. La única diferencia entre ambos preceptos estriba, rectamente, en el matiz que introduce a la necesidad de tener en cuenta el valor potencial de la información, lo cual, por demás, ya había sido advertido por nuestros autores[9]. Y como es doctrina asentada, el artículo 39.2 del ADPIC es de aplicación directa en nuestro país. Así lo prueban las decisiones de nuestros tribunales que lo han venido aplicando directamente desde hace más de una década para definir el concepto de secreto empresarial en sede del antiguo artículo 13 de la Ley 1/1991, de 1 de enero, de Competencia Desleal (en adelante «LCD»)[10]. La interpretación que la doctrina y, a su calor, la jurisprudencia ha ofrecido sobre los requisitos que deben darse cita en una información para constituir un secreto empresarial en el marco de ese precepto es, pues, plenamente trasladable a la nueva regulación, por lo que para su análisis detenido nos remitimos a ella[11].

Nuestro objetivo en los siguientes apartados será explorar si estos pueden concurrir en los datos y bajo qué condiciones.

1. Información y datos

La Directiva y la LSE exigen, ante todo, que el objeto susceptible de ser protegido como secreto empresarial sea «información»[12].

De acuerdo con Gal y Rubinfeld, la cadena de valor de los datos consta principalmente de 5 eslabones[13] de los cuales, a estos efectos, nos interesa destacar los siguientes tres: Recopilación, que consiste en la extracción, registro y

---

[8] A cuyo tenor: *Las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, en la medida en que dicha información a) sea secreta en el sentido de que no sea, como cuerpo o en la configuración y reunión precisas de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y b) tenga un valor comercial por ser secreta; y c) haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla*.

[9] *Vid*. MASSAGUER (1999), pág. 387; PORTELLANO (1997), pág. 345, y SUÑOL (2009), pág. 141.

[10] *Vid*. *ad ex*. entre las últimas, SSAP Barcelona 216/2021, secc. 15.ª, de 4 de febrero de 2021 [Ponente: José María Fernández Seijo] (ECLI: ES:APB:2021:400), Madrid 200/2020, secc. 28.ª, de 5 de junio de 2020 [Ponente: Francisco de Borja Villena] (ECLI: ES:APM:2020:6544), Pontevedra 387/2020, Secc.1.ª, de 30 de junio de 2020 [Ponente: Jacinto José Pérez Benítez] (ECLI: ES:APPO:2020:1244), Zaragoza 490/2020, Secc. 5.ª, de 4 de junio de 2020 [Ponente: Juan Carlos Fernández Llorente] (ECLI: ES:APZ:2020:987), Madrid 19/2019, secc. 28.ª, de 18 de enero de 2019 [Ponente: Enrique García García] (ECLI: ES:APM:2019:2366), Barcelona 1549/2019, secc. 15.ª, de 10 de septiembre de 2019 [Ponente: Luis Rodríguez Vega] (ECLI: ES:APB:2019:10731).

[11] *Vid*., por todos, PORTELLANO (1997), págs. 340-346; MASSAGUER (1999), págs. 384-391, FARRANDO (2001), pág. 104-147 y, ampliamente, SUÑOL (2009), pág. 105-239. Con anterioridad a la promulgación de la LCD y el ADPIC, *vid*. el análisis precursor que ofreció al respecto GÓMEZ SEGADE (1974), págs. 90-249 y espec. págs. 150-155 y pág. 188.

[12] No ignoramos que la LSE ha añadido también la referencia a «conocimientos», término ausente en la Directiva. No obstante, a nuestro juicio, esa adición es de dudosa compatibilidad con este último texto por dos razones. Primera, como hemos advertido, los Estados miembros no pueden desviarse de la noción de secreto empresarial establecida en la Directiva. Segunda, a mayor abundamiento, en aquel término se incluyen «conocimientos tácitos» y la Directiva excluye las «experiencias» adquiridas por trabajadores durante la prestación de sus servicios [*vid*. art. 1.3 letra *b)* de la Directiva].

[13] Este párrafo está basado en RUBINFELD y GAL (2019), págs. 746-747. A ello añaden el almacenamiento, que implica archivar datos en formas recuperables y su utilización que supone usar conocimientos basados en datos para predecir y tomar de decisiones en mercados relevantes.

agregación de datos en un formato apto para usarse en procesos de extracción de datos. Organización, que implica estructurar la base de datos e incluye la síntesis de ciertos puntos de datos u observaciones y la adición de encabezados y notas explicativas. Análisis, que comprende la integración y el procesamiento de diferentes tipos de datos.

Los dos últimos eslabones son los que transforman los datos en bruto («*raw data*»)[14] en información[15]. No existen, pues, particulares problemas en aceptar que los datos estructurados y contextualizados (*ad ex*. en una base de datos), los datos de entrenamiento o *corpus*[16] así como los que resultan de aplicar a estos últimos técnicas de análisis tales como el aprendizaje automático (*ad ex*. correlaciones entre puntos de datos, predicciones) pueden ser objeto de un secreto empresarial. Menos claro es, en cambio, que puedan serlo los datos en bruto[17]. Aunque inicialmente la Comisión Europea pareció admitir esa posibilidad[18], la definición de «datos» que contiene la Propuesta de Reglamento de datos parece decantarse por lo contrario pues, en ella, la información se concibe como especie de aquellos[19]. En la doctrina europea, no obstante, por lo general, se admite pacíficamente que los datos pueden *prima facie* protegerse como secreto empresarial estén o no estructurados o procesados[20]. En el bien entendido que lo eventualmente amparado es la «información» codificada en ese sistema binario (información semántica) y no las secuencias de bits y bytes (información sintáctica)[21]. Dada la importancia que en algunos sectores tienen los datos en bruto, seguramente este sea uno de los aspectos de la noción de secreto empresarial establecida en la Directiva respecto de los que Parlamento Europeo y la propia Comisión reclaman una aclaración[22].

Suele afirmarse que el legislador europeo no tuvo en consideración a los datos cuando promulgó la Directiva[23]. Aun siendo cierto, su Preámbulo contiene dos advertencias que permiten respaldar su inclusión. Primera, la importancia de formular una definición de secreto empresarial que no restrinja su objeto de

[14] Los datos en bruto son datos que no han sido procesados ni modificados tras su obtención (*ad ex*. el tráfico en Internet) *Vid*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «La Construcción de una Economía de los Datos Europea», Bruselas, 10 de enero de 2017, COM (2017) 9 final, punto 3.

[15] *Vid*. *idem* y Elkin-Koren y Gal (2018), pág. 410.

[16] Los datos de entrenamiento o *corpus* son los que se utilizan para entrenar al algoritmo y construir el modelo y son el resultado de un proceso muy costoso que llevan a cabo los analistas y que constan en esencia de las siguientes fases: en la primera, se recolectan y combinan datos que han sido medidos o se van medir y, en la segunda, estos se limpian; es decir: se identifican y corrigen problemas de calidad de los datos. *Vid*. *amplius*, Lehr y Ohm (2017), págs. 667-683.

[17] Conforme, Nordberg (2020), pág. 202.

[18] *Vid*., respectivamente, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 25 de noviembre de 2020 COM (2020) 760 final, pág. 16 y *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy*, SWD/2017/02 final, pág. 20.

[19] *Vid*. artículo 2.1 que define los datos como «toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual».

[20] *Vid*., entre muchos, Zech (2016), pág. 6; Kerber (2016); Surblytė (2016), págs. 8 y 9, pág. 5; Drexl *et al*. (2016), págs. 6-8; Drexl *et al*. (2016), págs. 268-269; Aplin (2017), págs. 65 y sigs.; Gómez Segade (2019-2020), pág. 151.

[21] Drexl *et al*. (2016), pág. 263.

[22] *Vid*. considerando 19.ª de la Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial.

[23] *Vid*., por todos, Drexl *et al*. (2016), pág. 268, y Wiebe (2017), pág. 65.

protección[24], lo cual sugiere que no hay razón para excluirlos. Segunda, la necesidad de no afectar a lo establecido en la actualmente derogada Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, sobre protección de datos personales[25], pues *a contrario* nos indica que los «datos» están comprendidos en su ámbito de protección.

2. El carácter secreto de los datos

Para que una información pueda merecer la condición de secreto empresarial es preciso obviamente que esta tenga carácter secreto. Y para determinarlo la LSE nos proporciona dos criterios: que no sea generalmente conocida y que no sea de fácil acceso por y para las personas que normalmente la utilizan[26].

La dificultad que para el círculo relevante extraña obtener la información por medios lícitos, que es a nuestro juicio el criterio más adecuado para determinar su naturaleza reservada[27], ha de medirse en función de los recursos cifrados en tiempo, dinero, esfuerzo o sencillamente ingenio que es necesario invertir a tal fin. Cuanto mayores sean, más probable será que la información no sea fácilmente accesible y a la inversa.

En el contexto que nos ocupa, su apreciación exige diferenciar entre datos individualmente considerados y conjuntos de datos (estructurados o no).

2.1. *Datos individualmente considerados*

Los datos aislados, sean técnicos (*ad ex*. datos generados por dispositivos) o de carácter personal (*ad ex*. búsquedas o compras realizadas por un individuo) rara vez quedarán cubiertos bajo el paraguas protector del secreto empresarial por una doble razón.

La primera radica en que tratándose de datos de carácter personal, el derecho de acceso y el derecho a la portabilidad de los datos que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, «el Reglamento de datos personales»), atribuye a los interesados (*vid*., respectivamente, arts. 15 y 20) podrían comprometer la posibilidad de conservarlos en secreto[28].

---

[24] *Vid*. considerando 14 de la Directiva.

[25] *Vid*. considerando 35 de la Directiva.

[26] *Vid*. artículo 1.3.*a)* de la LSE.

[27] *Vid*. *amplius* para el razonamiento que sustenta esta conclusión, Suñol (2009), pág. 122-133.

[28] Adviértase que ni el Reglamento de datos personales ni la Directiva de secretos empresariales se pronuncian de forma clara acerca de qué derecho (el derecho acceso y portabilidad de los datos de carácter personal o el derecho del titular del secreto a mantenerlos bajo reserva) prevalece en caso de conflicto. En efecto, los artículos 15.4 y 20.4 del Reglamento establecen que el derecho de acceso y el de portabilidad no deben afectar negativamente a los secretos empresariales, limitación, esta, que el considerando 63 parece extender también al artículo 15.1 y 15.3 del mismo texto. Por su parte, el considerando 35 Directiva de secretos empresariales declara que esta no debe afectar a los derechos y obligaciones previstos en la (ahora derogada) Directiva 95/46/CE sobre protección de datos personales y, en particular, y entre otros, el derecho del interesado de acceder a aquellos de sus datos personales que sean objeto de tratamiento. Por tanto, la resolución de este eventual conflicto, si acaso lo hay, solo puede determinarse atendiendo a las concretas circunstancias del caso [*vid*., en esta línea, Malgieri (2016), *passim*. Considera, en cambio, que tal conflicto no existe, Drexl *et al*. (2018), págs. 100-104.

La segunda y más poderosa razón estriba en que los datos individualmente considerados, cualquiera que sea su naturaleza, difícilmente gozarán de carácter secreto, pues a menudo son fáciles de obtener. Si, por ejemplo, un reloj inteligente permite identificar socavones en la acera, lo mismo pueden hacer las tecnologías de terceros. De hecho, es posible obtener los mismos datos de fuentes distintas (*ad ex*. los datos de localización pueden obtenerse desde dispositivos portátiles y de teléfonos inteligentes). Otro tanto puede decirse de los datos publicados en redes sociales abiertas y sin restricciones.

2.2. *Conjuntos de datos (incluidos los datos de entrenamiento)*

Un conjunto de datos puede constituir un secreto empresarial a pesar de que alguno o todos los datos individualmente considerados estén en el dominio público[29]. El sustento legal de esta afirmación se encuentra en la propia noción de secreto empresarial establecida en la Directiva y la LSE, que exige que la información «no sea generalmente conocida ni fácilmente accesible como cuerpo o en la configuración y reunión precisas de sus componentes» y, por tanto, con independencia de que los concretos elementos que lo integran individualmente atendidos tengan o no carácter reservado[30]. Lo determinante a estos efectos es que de la conjunción o articulación de todos los datos se configure un resultado que no sea fácilmente accesible a los sectores interesados reales o potenciales.

Es evidente que los conjuntos de datos de entrenamiento que se usan en el aprendizaje automático son de difícil acceso para el círculo de interesados[31]. Obtener la ingente cantidad de datos que se precisa al efecto (pues cuanto mayor es más fácil resulta descubrir correlaciones entre ellos) es muy costoso como lo es también medirlos y «limpiarlos». Además, esos datos pueden mantenerse internos y, por tanto, inaccesibles a los terceros, pues el programa de ordenador de aprendizaje automático los necesita como entrada (*«input»),* pero no requiere almacenarlos en su salida (*«ouput»);* esto es: en el algoritmo predictivo que genera[32].

Lo propio puede predicarse de la información que se obtiene tras procesarlos *(ad ex*. predicciones, correlaciones, agrupamientos). Y, también, de la que se obtiene tras aplicar otras técnicas de análisis, incluso cuando los datos de partida son públicamente accesibles.

Menos claras resultan ser las cosas para las compilaciones de datos que resultan de colectarlos de distintas fuentes. Si todas o algunas de estas fuentes son únicas —en el sentido de que los terceros no pueden acceder a ellas— y, por tanto, los son también los datos, no será fácil obtenerlas. No obstante, cuando los datos compilados son públicamente accesibles las probabilidades de que el conjunto tenga carácter secreto serán, por hipótesis, más reducidas. Ello no implica, por su supuesto, afirmar que la compilación no pueda ser como cuerpo o

[29] Es esta una idea mayoritariamente compartida. *Vid*. *ad ex*. Surblytė (2016), pág. 9; Aplin (2017), págs. 64 y sigs.; Sagstetter (2019), pág. 6.

[30] *Vid*. *amplius*, Suñol (2009), págs. 224-232. Lo advierte, también, Gómez Segade (2019-2020), pág. 152.

[31] *Vid*., en este sentido, Fromer (2019), págs. 723-724, y Hacker (2020), pág. 1032.

[32] *Vid*. Lehr y Ohm (2017), págs. 686 y sigs., y Fromer (2019), pág. 723.

en la reunión precisa de sus componentes en ningún caso de difícil acceso y, por ello, secreta[33]. Lo será, particularmente, cuando sea el resultado de seleccionar, combinar, depurar o contextualizar datos[34] y, en general, cuando su desarrollo requiera invertir una cantidad significativa de recursos y, por tanto, los operadores no puedan obtenerla paralelamente de forma fácil y poco costosa. En apoyo de esta conclusión cabe apelar a la jurisprudencia estadounidense, que en esas circunstancias ha considerado que las compilaciones y bases de datos controvertidas constituían un secreto empresarial[35].

3. El valor empresarial de los datos

El tercer requisito que el artículo 1.3 LSE exige a una información para constituir un secreto empresarial es que tenga valor empresarial, ya sea real o potencial, precisamente por ser secreta.

Es obvio que los datos no procesados e individualmente considerados si acaso tiene carácter secreto, no tienen valor, ni siquiera potencial, empresarial[36]. No obstante, con frecuencia se afirma que la concurrencia de este requisito suscita dudas incluso en conjuntos de datos por razón de la relación causa-efecto que, a tenor del precepto, ha de mediar entre el carácter secreto de la información y su valor. Especialmente —se dice— cuando los datos han sido recopilados a través de dispositivos y tienen naturaleza comercial. Y, también, cuando se procesan mediante técnicas de análisis que tienen un objetivo poco concreto, como sucede en aquellas que tratan de obtener correlaciones aleatorias en grandes cantidades de conjuntos de datos[37]. A nuestro juicio, sin embargo, un recto entendimiento de la exigencia de que la información tenga valor empresarial las despeja.

En efecto, la interrelación que media entre el carácter secreto de la información y su valor empresarial es, a nuestro juicio, *relativa*[38]. Ello implica que el legislador presume que, con carácter general, el valor de la información y, por ello, la ventaja competitiva que esta ofrece, proviene precisamente del hecho que sea secreta. Naturalmente, puede escaparse a sus consecuencias aportando indicios que, a la luz de las circunstancias del caso, demuestren que la información, aunque secreta, no proporciona ninguna ventaja competitiva a su titular[39]. No obstante, tratándose de conjuntos de datos, extravagantes serán en los que así suceda por las siguientes razones.

---

[33] Admiten esta posibilidad, entre otros SURBLYTĖ (2016), pág. 9, y DREXL *et al*. (2016), pág. 7.

[34] Conforme, SAGSTETTER (2019), pág. 6.

[35] *Vid*. *Experian Information Solutions, Inc*. *v*. *Nationwide Marketing Services Inc*., 893 F.3d 1176 (9th. Cir. *2018*), donde el tribunal concluyó que la compilación de nombres de consumidores asociados con sus direcciones tenía carácter secreto pues, aunque la actora obtenía ambos datos de fuentes disponibles públicamente, invertía recursos significativos para garantizar que estas eran certeras, seleccionando solo las que consideraba que tenían datos fiables, examinando nuevas fuentes potenciales y excluyendo los pares de nombres y direcciones que consideraba que no eran útiles para sus clientes, Además, resolvía conflictos entre fuentes de datos utilizando algoritmos para determinar qué información era correcta y, por lo tanto, podía incluirse en el CVD; *Compulife Software Inc*. *v*. *Newman*, 2020 WL 2549505 (11th. Cir. 2020), donde el tribunal concluyó —en un caso ciertamente dudoso— que, aunque las primas de seguros de vida contenidas en la base de datos controvertida individualmente consideradas no tenían carácter secreto pues eran fácilmente accesibles, en su conjunto aquella merecía la condición de secreto empresarial.

[36] *Vid*., no obstante, ZECH (2016), pág. 6.

[37] *Vid*. *ad ex*. DREXL *et al*. (2018), pág. 94, si bien el autor reconoce que el artículo 2.1 letra *a)* de la Directiva es lo suficiente flexible como para considerar que estos conjuntos de datos tienen valor empresarial.

[38] *Vid*., para esta idea y su desarrollo, SUÑOL (2020), *passim*.

[39] *Vid*. para algunos ejemplos, *idem*.

Primera, para dar por satisfecho el requisito que estamos examinando basta con que la información posea un valor empresarial «potencial». Por tanto, informaciones que todavía se encuentran en una fase inicial o de desarrollo pueden constituir un secreto empresarial. Tal es el caso, por ejemplo, de los conjuntos de datos que se usan para entrenar al algoritmo (de autoaprendizaje) y de aquellos en los que, mediante las oportunas técnicas de análisis, se extrae información valiosa (hallazgos) que a la postre permiten desarrollar nuevos productos o servicios o mejorar los existentes.

Segunda, la Directiva solo excluye del concepto de secreto empresarial, por carecer de valor empresarial, a las informaciones triviales o banales[40] (mal traducidas, por cierto, en la LSE como «informaciones de escasa importancia»). Si la trivialidad o insignificancia es el umbral mínimo del valor que aquellas han de poseer, convendrán en que pocas serán las que por esa razón queden excluidas de la protección jurídica del secreto empresarial. De hecho, no es fácil dar con ejemplos de informaciones que aun siendo secretas sean irrelevantes[41].

Finalmente, los casos en los que el legislador ha considerado que la información necesariamente tiene valor empresarial permiten respaldar que incluso los conjuntos de datos en bruto que han sido combinados de diversas fuentes lo tienen. Su divulgación, uso u obtención ilícita puede menoscabar los intereses económicos o la posición competitiva de su titular, que es circunstancia expresamente mencionada como determinante del valor empresarial de la información[42]. No en vano, los terceros pueden usarlos como punto de partida para extraer ulterior información.

De las consideraciones anteriores se desprende la conclusión de que los conjuntos de datos (estructurados o no) tienen valor empresarial actual o potencial, precisamente por ser secretos[43].

4. Adopción de medidas para mantener el carácter secreto de los datos

La última de las condiciones que la LES exige para calificar de secreto empresarial a una información (los conjuntos de datos) es que su titular haya adoptado medidas razonables para conservar su naturaleza reservada.

Si con carácter general consideramos que este requisito debe interpretarse de forma laxa para no socavar los incentivos que procura la protección jurídica del secreto empresarial[44], en el contexto que ahora nos ocupa nos parece imprescindible. La referencia a la necesidad de atender a las circunstancias del caso —que, por cierto, la LSE inexplicablemente ha omitido—[45] así lo permite. De otro modo, los titulares de los datos serán reacios a compartirlos, por ejemplo, mediante acuerdos de cooperación o colaboración o a través de *pools* entre empresas u otras entidades, justo el objetivo contrario al perseguido por la

[40] Esto es: las informaciones que en el *common law* y, especialmente en el Reino Unido y Australia, se han excluido tradicionalmente bajo el *nomen «trivial tittle-tattle»*; *Vid*., por todos, GURRY (2012), pág. 81.

[41] Lo advierten, también, BENTLY y SHERMAN (2018), pág. 1000.

[42] *Vid*. considerando 14 de la Directiva.

[43] *Vid*. Commission Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy.

[44] *Vid*., para el desarrollo, SUÑOL (2009), págs. 172 y sigs.

[45] Lo advierte, también, con ojos críticos, GÓMEZ SEGADE (2019-2020), págs. 154 y 155.

estrategia impulsada por la Comisión Europea. Por ello, el examen de la concurrencia de este requisito, a nuestro juicio, debe tener en cuenta las dos siguientes consideraciones.

La primera versa sobre las medidas de carácter jurídico que suelen requerirse al efecto y, en particular, sobre los pactos o acuerdos de confidencialidad. Con carácter general, su suscripción es esencial para mantener el carácter secreto de una información cuando el titular la comparte con otros sujetos. No obstante, tratándose de datos, en ocasiones, debido tanto al volumen y velocidad de los datos como a las largas cadenas de suministro y al gran número de participantes, exigirlos de forma exhaustiva puede ser impracticable.

La segunda de las consideraciones guarda relación con las medidas de protección técnicas (*ad ex passwords*, limitación de acceso, encriptación) y se orienta a advertir de que, con frecuencia, en su exigencia se mezclan incorrectamente dos planos que son muy distintos: las medidas de auto-protección que los operadores racionales deberían adoptar para proteger sus datos y las que legalmente se les ha de exigir para poder beneficiarse de la protección del secreto empresarial. Desde la primera perspectiva, su naturaleza, variedad y cantidad dependerán del tipo de riesgo de fuga o adquisición ilícita que los operadores deban afrontar. Desde la óptica jurídica, conviene ser flexible y requerir el mínimo indispensable para advertir a terceros del carácter secreto de los datos[46]. Cuestión distinta, claro está, es que si su titular los pone en circulación sin establecer medidas técnicas que limiten o impidan que los terceros accedan a ellos sin autorización (*ad ex*. encriptar la base de datos, establecer *passwords* de acceso), estos naturalmente carecerán de carácter secreto. Todo ello, sin perjuicio, de que, en tanto se manejen datos de carácter personal, sea preciso adoptar las medidas exigidas por la normativa de protección de datos de esa naturaleza, que nos son las mismas que las se requieren para que una información se proteja como secreto empresarial.

III. EL INCENTIVO A RECOLECTAR Y GENERAR DATOS QUE PROCURA SU PROTECCIÓN COMO SECRETO EMPRESARIAL

1. Planteamiento

Hasta donde nuestro conocimiento alcanza, no existen estudios empíricos que muestren de forma concluyente si es o no preciso estimular a los operadores a invertir recursos para obtener y generar datos[47]. Aunque enmarcado en el debate sobre su eventual protección mediante un derecho de exclusiva, algunos autores sostienen que en el caso de los datos no procesados (*raw data*) es innecesario en determinados sectores porque no existe un fallo de mercado debido a la ausencia de esos incentivos[48]. Es el caso, por ejemplo, de las plataformas digitales, para las que la recopilación de datos personales constituye el pilar de su negocio.

---

[46] *Vid*. SUÑOL (2009), págs. 185-190.

[47] Lo advierte, también, SCHEUERER (2020), pág. 21. En línea parecida, HARTMANN, ALLAN, HUGENHOLTZ, QUINTAIS y GERVAIS (2020), pág. 95, donde los autores reconocen que determinar si existe ese fallo de mercado requiere de un amplio estudio económico que queda fuera de su análisis.

[48] *Vid*. DREXL *et al*. (2016), págs. 273-276, y KERBER (2016), págs. 10 y 11, aunque este autor advierte que no puede descartarse que para algunos tipos datos, colectarlos y analizarlos requiera costes significativos y que es preciso realizar estudios específicos para determinarlo.

Con todo, existe cierto consenso en admitir que en diversos sectores la recolección, compilación y combinación de datos precisa invertir recursos financieros y/o esfuerzo y tiempo[49] (*ad ex*. en el sector automovilístico[50], en el de medicina personalizada[51], para los *data borkers*[52]). Y, también, en aceptar que, cualquiera que sea el sector de que se trate, generar conjuntos de datos de entrenamiento y modelos predictivos requiere normalmente de una inversión económica significativa[53]. Parece, pues, preciso preservar las inversiones realizadas por sus titulares e incentivarlos a seguir invirtiendo en la recopilación y generación de datos a futuro[54]. Así lo reconoce abiertamente la Propuesta de Reglamento de Gobernanza de Datos[55].

Los operadores suelen establecer medidas técnicas para tratar de impedir que terceros no autorizados puedan acceder a los datos. Y en sus transacciones, cada vez más frecuentes, cuyo objeto son datos (*ad ex*. contratos de licencia, *outsourcing*, *pools*, consorcios u otros acuerdos de colaboración), medidas jurídicas que someten a quienes acceden a ellos o los reciben al deber de mantenerlos en reserva y de no utilizarlos para el fin distinto del que se autorizó (*ad ex*. pactos o acuerdos de confidencialidad). Se diría, por tanto, que estos cuentan ya con medidas fácticas para proteger los datos y, por ello mismo, para resguardar las inversiones realizadas para recolectarlos y generarlos[56]. A nuestro juicio, sin embargo, estas medidas resultan insuficientes a tal fin, especialmente, por dos razones.

En primer término, las medidas técnicas que puedan establecerse no son infalibles y, en todo caso, es preciso estimular a los operadores a destinar sus esfuerzos a innovar en lugar de a eludirlas. La propia Comisión Europea ha destacado la necesidad de proteger los datos, especialmente los secretos empresariales, frente a su acceso ilícito, entre otras formas, mediante espionaje industrial[57].

En segundo término, las obligaciones de secreto o de limitación de su uso solo son exigibles a los sujetos sobre los que se proyectan, bien porque así lo

---

[49] *Vid*. para un estudio que muestra que, con carácter general, recolectar, organizar, almacenar y compartir algunos tipos datos es costoso Elkin-Koren y Gal (2019), págs. 350 y sigs. En esta línea de pensamiento pueden incluirse también a quienes con carácter general reconocen con la necesidad de incentivar a los operadores a invertir en la recopilación y generación de datos: *vid*. *infra* nota 52.

[50] *Vid*., por ejemplo, Mattioli (2018), págs. 287-288, que sostiene que los datos sobre vehículos son costosos de recopilar porque requieren el despliegue de vehículos en carreteras reales.

[51] *Vid*. *ad ex*., Price II (2015), págs. 437-442.

[52] *Vid*. Stepanov (2020), pág. 78, con ulteriores citas, quien mantiene que las empresas que recolectan y generan datos para intercambiarlos en el mercado (*data brokers*).

[53] Lo advierten, entre otros, Hacker (2020), págs. 1025 y 1033. Para un análisis del costoso proceso necesario para obtenerlos, Lehr y Ohm (2017), págs. 667-683, y Drexl *et al*. (2019), págs. 7-10.

[54] *Vid*., en este sentido, Rubinfeld y Gal (2017), pág. 374, quienes sostienen que por razón de la inexistencia de rivalidad en los datos pueden darse conductas de «*free riding*» que reduzcan la recompensa y, por tanto, el incentivo a invertir en la creación de bases de datos, Lohsse, Schulze y Staudenmayer (2017), págs. 15 y 16, quienes advierten de la importancia de asegurar una recompensa justa a los operadores que han creado las condiciones técnicas e invertido recursos en recolectar datos; Hacker (2020), pág. 1025, y Scheuerer (2020), págs. 25 y 26, quienes defienden el régimen de secreto protege las inversiones realizadas salvaguardando, así, el incentivo a innovar, con cita de Hilty, Hoffmann y Scheuerer (2020), pág. 21, Price II (2015), págs. 437-442, que señala que la recolección de datos en el sector de medicina personalizada reproduce el problema que subyace a otros bienes protegidos por la propiedad intelectual en sentido amplio, que los operadores no invierten lo suficiente porque, al no poder excluir de su uso a terceros, no pueden apropiarse plenamente de su valor, Hoffmann y Otero (2020), pág. 262, que señalan que los operadores precisan de algún tipo de protección fáctica que les sirva como incentivo a invertir en la generación de datos.

[55] *Vid*. Exposición de Motivos, punto 2, pág. 3.

[56] *Vid*. en esta línea, Drexl *et al*. (2016), pág. 3.

[57] *Vid*. considerando 15 de la Propuesta de Reglamento de Gobernanza de datos.

han asumido (*ad ex*. mediante un pacto confidencialidad), bien porque así se les exige legal o convencionalmente. Si estos las incumplen, el titular no puede, obviamente, hacer valer su incumplimiento frente a quienes de ese modo acceden a ellos para impedir que estos los divulguen o exploten ulteriormente. Teniendo en cuenta que los datos son por su naturaleza fáciles de reproducir y transferir es especialmente relevante que el titular cuente con algún mecanismo que le proporcione una protección más amplia de la que le brindan los diversos mandatos destinados a imponer un deber de reserva o de limitación de su uso.

Por esa razón, la protección de los datos del secreto empresarial constituye un instrumento necesario para incentivar su recolección y generación[58], pues colma esos huecos al reprimir tanto la obtención no autorizada de datos por medios ilícitos o reprobables (*vid*. *infra* 3.2) como la adquisición, revelación o uso de los datos por el llamado «adquirente indirecto», que es tercero no vinculado contractualmente con el titular (*vid*. *infra* 3.3).

2. Represión de la obtención ilícita o reprobable de datos

La LSE establece una lista de conductas que considera formas ilícitas de obtener un secreto empresarial si se realizan sin consentimiento y autorización del titular; a saber: mediante el acceso, apropiación y reproducción de los soportes que lo contienen o de los que se puede deducir como lo son, tal y como menciona el precepto a modo ejemplificativo, los documentos, objetos, materiales, sustancias o ficheros electrónicos [*vid*. art. 3 letra *a)* LSE]. Y completa ese catálogo con una cláusula general de prohibición de obtención ilícita de secretos empresariales [*vid*. art. 3 letra *b)* LSE].

Las conductas específicamente tipificadas en la LSE permiten reprimir, obviamente, los supuestos de obtención de datos más groseros que, en términos de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto, suponen un ataque contra los sistemas de información (*ad ex*. mediante el uso de claves de acceso ilegítimamente adquiridas, a través de robots o *bots* «maliciosos» y, en general, a través prácticas de *hacking*). Y también aquellos otros en los que el infractor exporta, transfiere y, en suma, reproduce de cualquier otro modo los datos almacenados en el ordenador, sistema informático o recurso de internet del titular a otros soportes o sistemas (*ad ex*. copiando los datos almacenados en un servidor interno a un dispositivo) así como los casos en los que aquel los obtiene mediante aparatos técnicos de transmisión, grabación o reproducción de la imagen o de cualquier otra señal de comunicación (*ad ex*. fotografiándolos, imprimiéndolos en papel, enviándolos por correo electrónico).

Por su parte, la cláusula general de prohibición de obtención de secretos empresariales, que reputa ilícita «cualquier otra actuación que, en las circunstancias del caso, se considere contraria a las prácticas comerciales leales», asegura que se considerarán ilícitas otras formas distintas de acceder a los datos que bien constituyen un ilícito en sí mismas (*ad ex*. inducir a un tercero a adquirirlos y/o

[58] *Vid*., por todos, los autores que sostiene que la protección jurídica del secreto empresarial incentiva la creación de nueva información y la innovación, entre nosotros, Gómez Segade (1981), pág. 211; Massaguer (1999), págs. 391-392; Suñol (2009), págs. 89-94 y, en la literatura extranjera también, por todos, Friedman, Landes y Posner (1991), págs. 61 y 64; Lemley (2008), pág. 2 y págs. 25-27. Así lo reconoce expresamente el legislador europeo en el Preámbulo de la Directiva (*vid*. considerandos 1-4).

revelarlos ilícitamente, servirse de un engaño para provocar en su titular o persona autorizada la decisión de confiarlos, comunicarlos o permitir su acceso) o son en todo caso reprobables (*ad ex*. captar los datos mediante drones, satélites y técnicas similares)[59].

3. Protección frente al adquirente indirecto de datos

El artículo 3.3 de la LSE tipifica como acto de violación de secretos empresariales su obtención, revelación o explotación por el llamado «adquirente indirecto»; esto es: quien obtiene y, en su caso explota o divulga posteriormente, un secreto empresarial de quien a su vez lo adquirió o, en todo caso, lo comunicó o usó ilícitamente, sabiendo o, en las circunstancias del caso, debiendo haber sabido de su origen ilícito[60].

Las conductas relevantes (obtención, revelación o explotación de un secreto empresarial) se delimitan, pues, en torno a un presupuesto objetivo y su ilicitud se halla condicionada a la concurrencia de un requisito subjetivo.

El presupuesto objetivo común a las conductas típicas es la violación de un secreto empresarial —los datos, por lo que ahora interesa— cometida por otro y no inducida a resultas de la cual el sujeto agente los obtiene directa o indirectamente y, en su caso, los divulga o explota después. Así, pues, aquel los obtiene bien de quien a su vez lo adquirió ilícitamente (*ad ex*. un *hacker*), pues esa ilicitud determina la deslealtad de su posterior revelación o explotación (*vid*. art. 3.2 LSE), bien de quien accedió a ellos lícitamente, pero incumpliendo al comunicarlo o usarlo su deber de reserva o cualquier obligación que limitaba su utilización (*ad ex*. un licenciatario de los datos) (*vid*. art. 3.3 en relación con el art. 3.2 LSE).

El requisito subjetivo al que la LSE condiciona la ilicitud de la obtención del secreto empresarial a raíz de su violación y, en su caso, su posterior divulgación o explotación, estriba en que en el momento de realizarlas el adquirente indirecto sepa o, en las circunstancias del caso, debiera haber sabido que aquel tenía un origen ilícito y, por tanto, que se divulgaba o explotaba ilícitamente.

Acreditar que el adquirente indirecto obtuvo, por lo que ahora importa, los datos secretos con conocimiento efectivo de su origen ilícito, salvo en casos groseros, no es sencillo en la práctica. Más halagüeño puede ser, quizás, demostrar que atendidas las circunstancias del caso aquel debiera haber sabido su origen ilícito o, lo que es lo mismo, que incumplió el deber de diligencia profesional que le era exigible al ignorarlo. Por supuesto, la determinación de este extremo dependerá de las circunstancias particulares de cada caso. Ello no obsta, sin embargo, a tener en cuenta alguna consideración de orden general. Es evidente que quien tiene interés en disponer de una información debe desplegar cierto esfuerzo en asegurarse de que puede acceder a ella sin infringir derechos de terceros. Pero, tratándose de secretos empresariales, cerciorarse de su propia existencia y de la identidad de su titular, en ocasiones, puede ser muy costoso.

[59] *Vid*., para un examen detenido de estos supuestos, Suñol (2009). págs. 319-326 y 354-362.

[60] *Vid*. *amplius* bajo el artículo 13 de la LCD, Suñol (2009), págs. 330-333. Advirtió, con anterioridad a la LCD, que el competidor que adquiere un secreto empresarial que otro obtuvo ilícitamente y lo sabe comete un acto de competencia desleal, Gómez Segade (1974), pág. 207.

Especialmente cuando de datos se trata. Por ello, esa obligación que el deber de diligencia impone no puede ser muy rigurosa. Lo contrario, aumentaría los costes de transacción y la aversión al riesgo de ser condenado por su obtención ilícita podría incentivar a los operadores a renunciar, por ejemplo, a suscribir acuerdos de colaboración con otras empresas. Todo la cual constituye una rémora para el intercambio y puesta en circulación de los datos. En particular, en los casos en los que el adquirente indirecto accede a ellos a cambio de precio (*ad ex*. a través de un contrato de licencia), que es lo más habitual en la práctica, por regla general esa obligación debe considerarse cumplida si el transmitente garantiza que los datos no infringen un secreto empresarial titularidad de un tercero. No obstante, esa garantía será insuficiente y el conocimiento sobre el origen ilícito de los datos secretos deberá entenderse presente si la identidad del transmitente o, entre otras circunstancias, el precio u otras condiciones pactadas alertaban claramente acerca de que aquellos eran un secreto empresarial que estaba siendo ilícitamente revelado. Un caso de estas características fue resuelto por el Noveno Circuito de Estados Unidos en el asunto que enfrentó a *Experian Information Solutions y Nationwide Marketing Services Inc*.[61]. En él, el tribunal concluyó que el bajo precio satisfecho por la compilación de datos considerada como secreto empresarial (menos del 1 por 100 de lo que se pagaba en el mercado por una licencia *one-time*) y su obtención «en propiedad» eran circunstancias bastantes para respaldar que el demandado tenía que haber sabido que los datos que obtenía tenía un origen ilícito.

IV. ACCESO, INTERCAMBIO Y USO DE DATOS QUE CONSTITUYEN UN SECRETO EMPRESARIAL

1. Planteamiento

Como hemos advertido al inicio, la Inteligencia Artificial y las tecnologías conexas dependen en gran medida de los datos. Dado el destacado papel que estos asumen en desarrollo económico, fomentar su acceso, uso, e intercambio se ha convertido en uno de los objetivos esenciales de la política estratégica de la Comisión Europea sobre economía de datos, dirigida a crear un mercado único digital que permita que estos fluyan libremente por la UE[62]. Muestra de ello es la Propuesta de Reglamento de gobernanza de datos cuyo propósito es, entre otros, fomentar su disponibilidad y uso, aumentando la confianza en los intermediarios de datos y reforzando los mecanismos para intercambiarlos[63].

La protección de los datos como secreto empresarial, a nuestro juicio, se adecúa razonablemente a este objetivo. Así, desde una óptica positiva, incentiva a los operadores a compartirlos (*vid*. *infra* 4.2). Y, desde una óptica negativa, no entraña una restricción innecesaria a su libre circulación gracias a la relación de supuestos de obtención, uso y revelación que ora se permiten ora se excep-

[61] *Vid*. *Experian Information Solutions v. Nationwide Marketing Services Inc*., 893 F.3d 1176 (9th. Cir. *2018*).

[62] *Vid*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos, Bruselas, 19 de febrero de 2020 COM (2020) 66 final.

[63] *Vid*. Exposición de Motivos, punto 1, pág. 1 de la Propuesta de Reglamento de gobernanza de datos.

túan del alcance sustantivo de la protección de los secretos empresariales[64] (*vid*. *infra* 4.2 y 4.3 respectivamente). Además, el mandato de proporcionalidad que establece al configurar las medidas de defensa frente a la violación de secretos empresarial permite atemperar algunos de los efectos en exceso gravosos que estas podrían entrañar para el infractor de los datos. Ese pudiera ser el caso de los remedios previstos respecto de las llamadas «mercancías infractoras», si acaso los datos pueden merecer esa calificación, cuestión que, como veremos, a nuestro parecer es bastante dudosa (*vid*. *infra* 4.4).

2. El incentivo a compartir datos

Para que los datos sean compartidos y obtenga un nivel óptimo de explotación es imprescindible que el titular pueda confiarlos a otros sujetos (colaboradores externos, clientes, socios en proyectos conjuntos, etc.) sin temor a que estos los revelen o exploten sin autorización o permitan a terceros aprovecharlos ilícitamente. De otro modo, los operadores tenderán a acapararlos, reorganizando su negocio de forma menos eficiente (*ad ex*. evitando la subcontratación), limitando su transmisión a los terceros (*ad*. *ex*. en forma de licencias, pools, *joint ventures*) e imposibilitando, en definitiva, la maximización de las ventajas que brindan.

La LSE reprime tanto la utilización o revelación de un secreto empresarial por quien al hacerlo incumple una obligación de secreto o de cualquier otra índole que limite su uso (*vid*. art. 3.2 de la LSE), como su obtención, uso o revelación por el «adquirente indirecto» (*vid*. art. 3.3 de la LSE). Al hacerlo, promueve la puesta en circulación de los datos y, con ello, su explotación eficiente, reduciendo la aversión de su titular a compartirlos con otros sujetos y asegurando, en consecuencia, su aprovechamiento eficiente[65]. No en vano la propia Comisión Europea ha advertido de que la falta de confianza en que las contrapartes cumplan sus compromisos contractuales es una de las razones que han impedido que las empresas intercambien datos con mayor frecuencia de la deseada[66].

Podría argumentarse, no obstante, que los diversos preceptos a través de los cuales nuestro ordenamiento impone a ciertos sujetos el deber de mantener bajo reserva determinadas informaciones secretas, sean de origen legal o convencional, ya son bastante para incentivar al titular de los datos a compartirlos. Hay razones, sin embargo, que permiten abrigar fundadas dudas. La primera ya ha sido advertida con anterioridad y radica en que ese deber no se proyecta sobre terceros. La segunda estriba en que el sistema de acciones que ofrece la LSE es mucho más robusto y eficaz. Es cierto que las cláusulas penales pueden disuadir a quienes están sometidos a un deber de reserva o a la obligación de no usar los datos para un fin distinto del que se autorizó a no divulgarlos o explotarlos sin autorización. Pero no siempre se introducen en los correspondientes contratos.

---

[64] Conformes, entre otros, Drexl *et al*. (2018), pág. 92; Aplin (2017), pág. 70; Leistner (2020), pág. 18.

[65] *Vid*. entre los autores han defendido que la protección jurídica del secreto empresarial incentiva su puesta en circulación y maximiza su explotación, Suñol (2009), págs. 98-99; Lemley (2008), pág. 3 y págs. 29-35. También la Directiva reconoce este extremo (*vid*. considerandos 3 y 8).

[66] *Vid*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos, Bruselas, 19 de febrero de 2020 COM (2020) 66 final, pág. 8.

3. Licitud de la obtención, uso o revelación de los datos

A diferencia del artículo 39 del ADPIC y de lo que sucedía en el antiguo artículo 13 de la LCD, la LSE ha establecido expresamente la licitud, entre otras conductas y por lo que ahora interesa destacar, de la obtención de secretos empresariales de forma independiente o mediante ingeniería inversa. Y ha completado ese listado con una cláusula general por la que se reputa lícita cualquier otra práctica que, en las circunstancias del caso, sea conforme con las prácticas comerciales leales. Huelga decir que sentada la licitud de la obtención de los datos secretos, lícita será también, desde la óptica de la LSE, su ulterior divulgación y explotación.

3.1. *Obtención independiente de datos*

La licitud de esta conducta posibilita que los terceros puedan obtener o desarrollar de forma autónoma los mismos datos y, posteriormente, explotarlos o divulgarlos sufragando los costes de su obtención o creación. Ello es especialmente relevante tratándose de datos que son públicamente accesibles (*ad ex.* datos que diversos dispositivos pueden obtener en tiempo real). Y, también, de compilaciones compuestas simplemente de datos, aunque sea recolectados de distintas fuentes, que tienen esa misma naturaleza, pues los terceros pueden desarrollarlas y explotarlas sin temor a afrontar una demanda por violación de secretos empresariales.

No puede ignorarse, sin embargo, que a veces los conjuntos de datos son difíciles de obtener de manera independiente. Muchas empresas no disponen de los vastos recursos que se requieren para adquirirlos o generarlos. Además, en ocasiones los operadores se sirven de otros recursos que hacen materialmente imposible —o casi— obtenerlos. Un ejemplo ilustrativo de ello son las patentes consistentes en tecnologías cuya puesta en práctica genera datos valiosos[67]. Durante su vigencia cuanto menos, recrear esos datos de forma independiente tiene un coste casi prohibitivo[68]. La patente denominada «*PageRank*» de la que hasta hace bien poco era titular Google, es buena muestra. A través de ella, Google compiló infinidad de datos sobre ubicaciones, preferencias, consultas, datos personales, etc., de los usuarios que el resto de competidores no pudieron obtener durante la vigencia de la patente. Es más, en la medida en que los ha mantenido en secreto, ello le ha permitido obtener una ventaja competitiva más allá de la expiración de la patente, toda vez que los ha usado, a su vez, para mejorar las búsquedas realizadas por los usuarios o enviar publicidad adaptada a cada uno de ellos[69]. Debe advertirse, con todo, que el problema en estos casos no estriba tanto en que los datos se mantengan en secreto, cuanto en que puedan patentarse esta clase de invenciones que los producen en primer lugar.

---

[67] *Vid.,* sobre esta clase de invenciones, SIMON y SICHELMAN (2017), *passim,* y circunscrito a invenciones relacionadas con pruebas de diagnóstico médico, BURK (2015), *passim*.

[68] *Vid.,* entre quienes lo señalan, BURK (2015), págs. 248-249; SIMON y SICHELMAN (2017), págs. 380 y 410.

[69] Advierten con ojos críticos de este efecto respecto de esta clase de invenciones en general, SIMON y SICHELMAN (2017), págs. 413 y sigs. En la misma línea, respecto invenciones sobre pruebas de diagnóstico, BURK (2015), págs. 249 y sigs., si bien este autor observa también un efecto positivo consistente en que esta clase de invenciones permiten agregar datos valiosos que están dispersos y que, de otro modo, resultarían inservibles.

3.2. *Obtención de datos mediante ingeniería inversa*

El artículo 2.1.*b)* LSE faculta a obtener el empresarial mediante ingeniería inversa; esto es: a través de la observación, estudio, desmontaje o ensayo del producto u objeto que lo contiene o en que consiste.

Teóricamente, la declarada licitud de esta conducta está orientada a propiciar que los terceros puedan, por ejemplo, obtener los datos del producto lícitamente adquirido que los contiene (*ad ex*. un dispositivo, un programa de ordenador). Y ello, incluso cuando para hacerlo eludan o destruyan las medidas técnicas de seguridad que el titular haya incorporado para impedirlo. En la práctica, sin embargo, cuando de datos se trata, no es muy prometedora por una doble razón.

De entrada, la LSE permite, por imposición de la Directiva, que su titular pueda prohibir la ingeniería inversa a través una cláusula contractual válida, lo cual, dado el destacado papel que aquella asume en el progreso tecnológico[70] resulta desde una óptica económica tan sorprendente como reprochable[71]. Al respecto, basta advertir que, salvo en el ámbito de los programas de ordenador, cuya normativa impone restricciones importantes a la posibilidad de pactar este tipo cláusulas[72], supone dejar al arbitrio del titular del secreto el que los terceros puedan ponerla en práctica y, por ello mismo, vaciar completamente de contenido su licitud. Las cláusulas que prohíben el uso de sistemas automatizados o de *software* para extraer datos, por ejemplo, de una página web («*screen scraping*»), cuya licitud ha sido bendecida por el TJUE, son un magnífico ejemplo[73]. Su única virtud, si acaso, es que faculta a los titulares a prohibir que terceros puedan analizar los datos «hacia atrás» para «des-anonimizarlos».

Pero aun cuando no exista una cláusula que prohíba la realización de ingeniería inversa, no puede obviarse que en algunos casos es muy costoso obtener los datos a través de esa técnica. Así sucede, por ejemplo, en el aprendizaje automático. Los datos no pueden discernirse del programa de ordenador basado en esa técnica y puesto en el mercado, por la sencilla razón de que no están contenidos en él y los modelos predictivos y algoritmos desarrollados sobre la base de esos datos son muy complejos y difícilmente permiten obtener los datos de entrenamiento introducidos[74]. Otro tanto, ocurre con las patentes consistentes en tecnologías cuya puesta en práctica genera datos mientras estas se hallan en vigor[75].

3.3. *La cláusula general de licitud de obtención de datos secretos*

El artículo 2.1 letra *d)* de la LSE contiene una cláusula general de licitud de formas de acceder al secreto empresarial. De acuerdo con ella se consi-

[70] *Vid*., por todos, SAMUELSON y SCOTHMER (2002), *passim*.

[71] *Vid*., para otra opinión, DREXL *et al*. (2018), pág. 97, quien ve con buenos ojos que la Directiva permita prohibir mediante una cláusula contractual válida la ingeniería inversa para impedir que puedan eludirse medidas protección puestas por fabricante para que pueda accederse a los datos almacenados en un dispositivo.

[72] *Vid*. artículos 6 y 8 de la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril, sobre la protección jurídica de programas de ordenador y artículo 100.5 LPI.

[73] *Vid*. case C-30/14 *Ryanair Ltd v. PR Aviation BV* [2015] (ECLI: EU:C:2015:10).

[74] *Vid*., para la explicación, FROMER (2019), pág. 723, con ulteriores citas. Advierten también que en ciertos casos es muy costo obtener los datos de entrenamiento, DREXL *et al*. (2019), pág. 10.

[75] Lo advierten SIMON y SICHELMAN (2017), págs. 407-409.

dera lícita toda conducta que sea conforme con las prácticas comerciales honestas.

La adecuación del modo de obtener un secreto empresarial (los datos) al criterio de licitud establecido en esta cláusula general solo puede determinarse en atención a las circunstancias del caso. Los tribunales tienen, por tanto, un margen considerable para amoldar su enjuiciamiento al contexto de los datos. Ello no impide, sin embargo, reconocer algunos supuestos ilustrativos de conductas que, a nuestro juicio, quedan comprendidas en ella.

Es el caso, por ejemplo, de la obtención de los datos secretos por quien, en el momento que entró en su conocimiento, no sabía ni debiera haber sabido su origen ilícito y, por tanto, de buena fe (*vid*. art. 8 LSE). En efecto, como se sigue claramente de una lectura *a contrario* del apartado primero y segundo del artículo 3 de la LSE, esta conducta no constituye una violación de secretos empresariales. Correlato de ello es que la ulterior explotación o divulgación de los datos así obtenidos tampoco puede reputarse ilícita. En consecuencia, frente a esas conductas no cabe solicitar ninguno de los remedios previstos en la LSE. Estos solo proceden si en el momento de realizarlas quien obtuvo los datos a raíz de su divulgación o explotación ilícita tenía conocimiento (efectivo o debido) de ese origen ilícito, puesto que ello supone, en cambio, una violación de secretos empresariales (*vid*. art. 3.3 en relación con el art. 8 de la LSE).

Lo propio puede decirse cuando se accede a los datos accidentalmente o a consecuencia de un error (*ad. ex*. se reciben por correo a resultas de una equivocación del titular). Pueden trasladarse, pues, aquí las consideraciones que acabamos de realizar sobre su obtención de buena fe.

Finalmente, también pueden considerarse conformes con las prácticas honestas algunas formas de acceder a los datos que cuentan con una causa justificada que la legitime como, por ejemplo, desencriptarlos sin consentimiento del titular cuando hay una amenaza de infección de un virus, u obtenerlos para comprobarlos y tomar las medidas oportunas para afrontar ese virus u otras amenazas potenciales.

4. Acceso, revelación y uso de datos en supuestos exigidos o permitidos por la Ley

La obtención, utilización o revelación de un secreto empresarial y, por ende, de los datos que tienen esa condición, es lícita en los casos en los que la ley lo exija o cuando lo permita (*vid*. art. 2.2 de la LSE).

Y es que, en efecto, nuestro ordenamiento está plagado de normas que obligan a ciertos sujetos a comunicar y, con menos frecuencia, a acceder o explotar informaciones que pueden constituir un secreto empresarial, en cuyo caso y como es obvio, tales conductas no constituyen una violación de los mismos. De hecho, los supuestos que el legislador español ha añadido en la letra *d)* del artículo 3.2 LSE para ilustrar cuándo la obtención, divulgación o explotación de un secreto empresarial tiene un fin legítimo y, por tanto, es lícita, ya están contemplados en nuestro ordenamiento[76] y, por ello mismo, amparados por el artículo 2.2 LSE.

[76] *Vid. ad ex*. el artículo 39.1 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, el artículo 18 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, los artículos 93 y 94 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Además, este precepto asegura que no se reprimirán conductas que están autorizadas, explícita o implícitamente, tanto por la propia LSE como por otras normas internas o comunitarias. La toma de postura del legislador obliga a que no constituyan una violación de secretos empresariales. Especialmente relevante en este contexto es toda legislación europea sectorial que se ha promulgado sobre el acceso a los datos en determinados ámbitos (*ad ex*. el sector de la automoción, los proveedores de servicios de pago, la información en materia de medición inteligente, los datos de la red eléctrica)[77]. Y también los actos amparados por alguna de las excepciones previstas en legislaciones específicas como es el caso, por ejemplo, del Derecho *sui generis* sobre los programas de ordenador y las bases de datos[78].

A todo ello cabe añadir una virtualidad ulterior especialmente importante en el ámbito que nos ocupa: el artículo 2.2 de la LSE asumirá como lícitas todas aquellas formas de acceder, usar o divulgar datos que el legislador nacional o europeo decida permitir o exigir a futuro. Valga como botón de muestra la facultad que el artículo 5 de la Propuesta de Gobernanza de datos brinda a los organismos del sector público de permitir la reutilización de datos de carácter no personal en determinados supuestos y bajo ciertas condiciones. Y también, la obligación que el artículo 6 letra *i)* de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de mercados digitales)[79] impone a los llamados «guardianes de acceso» de permitir a los usuarios profesionales, o a terceros autorizados por este, el acceso y el uso efectivos, de alta calidad, continuos y en tiempo real de los datos agregados o no agregados en las circunstancias allí establecidas.

5. Excepciones a la violación de datos

El artículo 2.3 de la LSE establece un listado de supuestos de obtención, revelación, y explotación que se excepcionan del alcance de la protección jurídica del secreto empresarial y frente a los cuales no proceden, pues, las medidas, procedimientos y recursos previstos en el mismo texto. En verdad, todos ellos son especie del último que se relaciona; esto es: obtener, revelar o usar un secreto empresarial con el fin de proteger un interés legítimo reconocido por el Derecho de la Unión o nacional [*vid*. art. 2.3 letra *d)* de la LSE], como prueba la experiencia inglesa, de donde sin duda proviene el artículo 5 del Directiva (el precepto análogo al art. 2.3 de la LSE), que tradicionalmente ha englobado esos supuestos en la llamada *public interest defense*[80]. No obstante, en aras de dejar en claro su licitud, el legislador europeo ha optado por desmembrarlas.

De entre ellos, merecen especial atención tantos los supuestos comprendidos en el artículo 2.3 letra *d)* de la LSE que acabamos de mencionar como los englobados en la letra *b)* del mismo artículo (esto es: cuando las conductas se

[77] *Vid*., respectivamente, *DO* L 188, de 18 de julio de 2009, pág. 1, modificado por *DO* L 151, de 14 de junio de 2018, pág. 1; *DO* L 337, de 23 de diciembre de 2015, pág. 35; *DO* L 158, de 14 de junio de 2019, pág. 125, y *DO* L 211, de 14 de agosto de 2009, pág. 94.

[78] *Vid*., respectivamente, artículo 100.5 y 34 LPI.

[79] *Vid*., particularmente, artículo 6 letras *h), i)* del Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de mercados digitales), Bruselas 15 de diciembre de 2020, COM (2020) 842 final.

[80] *Vid*., por todos, Gurry (2012) pág. 327 y 346.

realizan con la finalidad de descubrir, en defensa del interés general, alguna falta, irregularidad o actividad ilegal)[81].

5.1. *Conductas realizadas con el fin de descubrir, en defensa del interés general, una falta, irregularidad o actividad ilegal*

Como nuestra doctrina ya había advertido bajo el marco del artículo 13 LCD, si la información objeto del secreto empresarial versa sobre actuaciones constitutivas de delito o de ilícitos de otra naturaleza (*ad. ex.* infracciones civiles, administrativas o financieras) su comunicación no supone un acto de violación de secretos empresariales[82]. En realidad, esta no constituye tan siquiera un incumplimiento del deber de secreto que pudiera pesar sobre quien los rebela pues, obviamente, ese deber no abarca la obligación de silenciar actuaciones ilegales. De ahí que la LSE aparte estas conductas del ámbito de la protección que ofrece el secreto empresarial. De hecho, como hemos visto, no faltan preceptos en nuestro ordenamiento que obligan a poner en conocimiento de las autoridades competentes hechos o conductas que pudieran constituir una infracción de la normativa correspondiente o denunciar o comunicar actividades delictivas[83]. Además, si la información versa sobre una infracción comprendida en el ámbito objetivo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (en adelante, «La Directiva 2019/1937»), su revelación ha de entenderse permitida por el Derecho de la Unión y, por ello, asimismo lícita a la luz de artículo 2.2. de la LSE siempre que se cumplan las condiciones establecidas en aquella (*vid.* considerando 98 y art. 21.7 *in fine* de la Directiva 2019/1937).

Así pues y como muestra, los trabajadores u otros colaboradores del titular de los datos pueden revelar cualquier irregularidad, fraude o, en general, actuación ilícita relacionada con los datos cometida por su principal (*ad ex.* una infracción de la normativa de protección de datos de carácter personal, un supuesto de discriminación contrario al art. 18 CE). Más difícil encaje tiene, a nuestro juicio, la obtención o explotación de datos realizadas con ese fin, pese a que, *prima facie,* la LSE también las reputa lícitas.

Cuestión distinta es que, atendido que esta clase de conductas se justifican y toleran por razón de su interés general, el modo en el que se lleva a cabo la revelación y, especialmente, la persona u organismo escogido para realizarla son factores que, a nuestro juicio, han de tomarse en consideración a estos efec-

---

[81] A nuestro juicio, *la excepción contemplada en la* letra *a)* del artículo 3.2 LSE (*esto es:* obtención, revelación o explotación de secretos empresariales en ejercicio de la libertad de expresión e información) se haya especialmente dirigida a los medios de comunicación a fin de permitir, como señala el considerando 19.º de la Directiva, el periodismo de investigación y la protección de las fuentes periodísticas [*vid.,* sobre este extremo, bajo el artículo 13 de la LCD, Suñol (2009), págs. 435-440]. En todo caso, para un buen análisis de las razones que explican por qué ese derecho fundamental es poco prometedor fuera de ese marco, en Estados Undios, Samuelson (2011), *passim*.

[82] Sobre esta conducta bajo el artículo 13 de la LCD, Suñol (2009), págs. 442-449. Bajo otra aproximación, advirtió con anterioridad a la LCD que esta clase de informaciones no pueden constituir un secreto empresarial por ausencia de un interés legítimo en proteger el secreto, Gómez Segade (1974), págs. 238 y sigs.

[83] *Vid.,* con carácter general, artículos 259, 262 y 264 LECrim. *Vid.,* con carácter más específico como ejemplo, artículo 18 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

tos. La salvaguarda de ese interés no precisa en todo caso que la información se difunda al público en general (*ad ex*. divulgándolos en la prensa). De ahí que parezca razonable sostener que, por regla general, tan solo pueden entenderse comprendidas en esta excepción las comunicaciones efectuadas a la entidad u autoridad adecuada o facultada para actuar[84]. Esta es, de hecho, la posición que el legislador europeo ha acogido en la Directiva 2019/1937, puesto que, de acuerdo con lo dispuesto en su artículo 15, las personas que revelen públicamente la información sobre una infracción comprendida en su ámbito de aplicación solo pueden acogerse a la protección que esta dispensa en circunstancias muy excepcionales específicamente identificadas en ese precepto.

5.2. *Interés legítimo que justifica la violación de los datos*

La obtención, revelación o uso de un secreto empresarial puede estar justificada por otros intereses legítimos reconocidos por el Derecho europeo o español. Es esta una fórmula de contornos abiertos que permite ahormar un abanico amplio de supuestos que abarcan desde la necesidad de salvaguardar bienes constitucionalmente protegidos (*ad ex* la salud pública, el medioambiente o la defensa de la seguridad nacional) como, potencialmente y por lo que ahora interesa destacar, proporcionar una explicación sobre una decisión algorítmica al interesado a los efectos del Reglamento de datos personales, o revelar los datos de entrenamiento sobre los que se ha construido el algoritmo y sobre los que se considera que existe un problema de sesgo[85]. Más dudoso es si la necesidad de preservar la competencia como institución puede considerase un interés legítimo a estos efectos, lo cual devendría especialmente relevante en el marco de la economía de datos.

6. El mandato de proporcionalidad: remedios frente a las llamadas «mercancías infractoras»

Finalmente, para determinar las medidas que se acuerden por virtud de las acciones previstas en la LSE contra los infractores de secretos empresariales el legislador obliga a atender al principio de proporcionalidad (*vid*. arts. 9.3 y 22 de la LSE). Este mandato reviste gran importancia pues faculta al juzgador bien a denegar algunas de las solicitadas por el titular de los datos (a excepción del remedio indemnizatorio) contra sus infractores, bien a flexibilizar su contenido. Su papel puede ser especialmente relevante a la hora de configurar, llegado el caso, los remedios previstos de forma específica frente una modalidad de utilización de secretos empresariales; a saber: la producción, oferta o comercialización, importación, exportación o almacenamiento con tales fines de las llamadas «de mercancías infractoras» (*vid*. art. 3.4 de la LSE). Y, en particular, la prohibición de fabricarlas, ofrecerlas, comercializarlas, utilizarlas, importarlas, exportarlas o almacenarlas con tales fines, la aprehensión de las mercancías y de los medios destinados únicamente a su producción, así como su atribución

[84] *Vid*., sobre este extremo, Suñol (2009), págs. 448-449.

[85] *Vid*., en esta línea, entre otros, Katyal (2019), pág. 126. Y por todos los que advierten y explican los problemas de sesgo que pueden producirse al desarrollar los datos de entrenamiento, Lehr y Ohm (2017), *passim*.

en propiedad al demandante [*vid*. art. 9.1 letras *c), d)* y *f)* de la LSE][86]. Diversos son los autores que han advertido de que, tratándose de datos, este supuesto de violación de secretos empresariales puede restringir excesivamente su libre circulación[87].

Con todo, a nuestro juicio, es muy dudoso que los conjuntos de datos puedan considerase «mercancías» a los efectos del artículo 3.4 de la LSE, definidas como, lo están, como productos y servicios cuyo diseño, características, funcionamiento, proceso de producción, o comercialización se benefician de manera significativa de secretos empresariales obtenidos, utilizados o revelados de forma ilícita[88]. El término «producto» al que alude el precepto parece circunscribirlas a algo que ha sido fabricado. Lo mismo cabe decir de la información que resulta de procesar esos conjuntos de datos. Además, el sujeto que realiza las conductas relevantes no es, a nuestro juicio, quien utiliza propiamente el secreto empresarial (en nuestro caso, los datos). Se trata de un tercero que bien desarrolla un producto o presta un servicio que incorpora a otro que fue fabricado o prestado utilizando ilícitamente un secreto empresarial (*ad ex*. un producto complejo, como pudiera serlo un kit de diagnóstico, en el que uno de sus componentes ha sido desarrollado usando un secreto empresarial), bien ofrece, comercializa, importa, exporta o almacena con tales fines un producto o servicio que fue desarrollado (por otro) usando ilícitamente un secreto empresarial. Finalmente, el requisito subjetivo al que condiciona la ilicitud de las conductas, que es idéntico al que se exige al «adquirente indirecto», permite al menos excluir a quienes no tenían conocimiento (efectivo o debido) de que los datos que incorpora la mercancía se habían utilizado ilícitamente.

V. CONCLUSIÓN

El acceso, uso e intercambio de datos es fundamental para el desarrollo de la Inteligencia Artificial y otras tecnologías conexas vitales para el crecimiento económico. Pero, naturalmente, cuando recolectarlos y generarlos es costoso las empresas han de contar con incentivos adecuados para hacerlo en primer lugar.

El sistema de protección jurídica del secreto empresarial establecido en la LSE, a diferencia de lo que sucede con los derechos de propiedad intelectual *strictu sensu*, no otorga a su titular un derecho de exclusión que pueda oponer *erga omnes*. Así se sigue especialmente del conjunto de supuestos de acceso, uso o revelación del secreto empresarial que bien estima lícitos, bien excepciona de su alcance de protección. Además, obliga a tener en cuenta numerosas circunstancias e intereses legítimos al configurar los remedios frente a su violación. No obstante, a través de las conductas que reprime proporciona al titular del secreto empresarial una ventaja suficiente en términos de *lead time* o costes relativos.

Este particular engranaje de conductas que prohíbe y permite, unido a la flexibilidad con la que pueden modelarse las medidas de defensa, hace que este

[86] *Vid*., sobre la acción de atribución en propiedad de mercancías infractoras de un secreto empresarial, PASTOR (2020), *passim*.

[87] *Vid*. *ad ex*. DREXL (2018), pág. 99, y LEISTNER. (2020), pág. 20.

[88] Advierte, no obstante, que los términos «bien» y «*produkt*» al que respectivamente aluden la versión francesa y Alemania pueden incluir «bienes digitales», DREXL *et al*. (2018), pág. 99.

sistema sea, a nuestro juicio, especialmente adecuado para proteger datos que merezcan la condición de secreto empresarial —que, como hemos visto, no son todos— toda vez que: i) estimula a los operadores a invertir en recolectarlos y generarlos, ii) no distorsiona innecesariamente su libre circulación. A esta última conclusión podría objetarse que la protección de los datos como secreto empresarial faculta a su titular a impedir que terceros accedan a ellos y los usen en un abanico nada desdeñable de supuestos. Por tanto —seguiría el argumento— tiene el potencial de obstaculizar su libre flujo. A nuestro juicio, sin embargo, esta objeción pasa por alto las siguientes consideraciones.

Primera, respecto de quienes acceden lícitamente a los datos, la LSE reprime su uso y divulgación en circunstancias no muy distintas de las que los operadores alcanzan mediante la celebración de contratos y adopción de medidas técnicas, con la ventaja de que permite reprimir otro tanto a quienes no vinculados contractualmente. Y en todo caso, tanto respecto de estos últimos como de los primeros faculta al juez a amoldar los remedios frente su violación atendiendo a los intereses en juego, que bien pueden saldarse, por ejemplo, en la sustitución la cesación por una compensación económica.

Segunda, determinar sí y, en su caso, en qué condiciones resulta oportuno permitir que terceros accedan a los datos requiere de un balance juicioso entre el valor social que resulta de ello, los intereses empresariales legítimos de las empresas y la necesidad de proteger la privacidad de los usuarios. La posibilidad de acceder y usar datos y el espectro de modalidades de ese acceso y uso no puede ser idéntico para entidades públicas, empresas, investigadores o particulares. De hecho, tratándose de contrapartes o competidores no faltan estudios económicos que cuestionan o niegan que sea eficiente obligar a los titulares de datos a compartirlos[89]. El sistema de protección jurídica del secreto empresarial es, en este sentido, neutral. No obstante, es poroso; asume las opciones que al respecto adopte el legislador en otras normas generales o sectoriales, permitiendo el acceso, uso o divulgación de los datos cuando estas así lo autoricen o, en su caso, impongan.

Finalmente, obvio es decirlo: la conducta del titular de los datos que constituyen un secreto empresarial y, por ende, la facultad de impedir que los terceros accedan a ellos, no está exenta de sujetarse a los límites generales que resultan tanto de las exigencias generales de la buena como de las normas de defensa de la competencia.

VI. BIBLIOGRAFÍA

APLIN, Tanya (2017), «Trading Data in the Digital Economy: Trade Secrets Perspective», en LOHSSE, S.; SCHULZE, R., y STAUDENMAYER, D. (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools*, C. H. Bert-Hart Publishing-Nomos, Germany-New York-United Kingdom, págs. 59-71.

[89] Diversos son los estudios económicos que lo cuestionan o niegan. *Vid. ad ex.* ELKIN-KOREN y GAL (2019), págs. 430-431, quienes muestran que obligar a los operadores a intercambiar los datos (una vez recolectados) no es una solución eficiente porque podría reducir la cantidad y la calidad de los datos recogidos a un nivel socialmente sub-óptimo, METZGER (2020), *passim*, espec. pág. 14, quien concluye que la imposición de una obligación de carácter general de permitir el acceso y portabilidad de los datos recogidos y procesados por una de las partes contratantes durante un contrato B2B difícilmente puede justificarse atendiendo a modelos consolidados de análisis económico de los contratos.

BALKIN, Jack M. (2017) «The Three Laws of Robotics in the Age of Big Data», *Ohio State Journal* 78, págs. 2017-1241.

BENTLY, Lionel, y SHERMAN, Brad (2018), *Intellectual Property Law*, *Intellectual Property Law,* University Press, Oxford.

BURK, Dan L. (2015), «Patents As Data Aggregators in Personalized Medicine», *Boston University Journal of Science and Technology Law* 21, *UC Irvine School of Law Research* Paper No. 2015-47, págs. 233-255.

DREXL, Josef (2017), «Designing Competitive Markets for Industrial Data-Between Propertisation and Access», *JIPITEC* 8, págs. 257-292.

— (2018), «Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organization», *BEUC*, Bruselas, págs. 1-168. Accesible en *https://www.ip.mpg.de/fileadmin/ipmpg/content/aktuelles/aus_der_forschung/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf*.

DREXL, Josef; HILTY, Retro; DESAUNETTES, Luc; GREINER, Franciska; KIM, Daria; RICHTER, Heiko; SURBLYTĖ, Gintare, y WIEDEMANN, Klaus (2016), «Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition», *Max Planck Institute for Innovation and Competition Research Paper* 16-10, págs. 1-12.

— (2019), «Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective», Max Planck Institute for Innovation & Competition Research Paper No. 19-13. Accesible en SSRN: *https://ssrn.com/abstract=3465577*, págs. 1-15.

ELKIN-KOREN, Niva, y GAL, Michal S. (2019), «The Chilling Effect of Governance-by-Data on Data Markets», *The University of Chicago Law Review* 83, págs. 403-431.

FARRANDO, Ignacio (2001), *El deber de secreto de los administradores de sociedades anónimas y limitadas,* Civitas, Madrid.

FRIEDMAN, David D.; LANDES, William M., y POSNER, Richard A. (1991), «Some Economics of Trade Secret Law», *Journal of Economics Perspectives* 5, págs. 61-72.

FROMER, Jeanne C. (2019), «Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation», *New York University Law Review* 94, págs. 706-727.

GAL, Michal S., y RUBINFELD, Daniel L. (2019), «Data Standardization», *New York University Law Review* 94, págs. 738-769.

GÓMEZ SEGADE, José Antonio (1974), *El Secreto industrial (Know-How): concepto y protección*, Tecnos, Madrid.

— (1981) «Algunos aspectos de la licencia de Know-How», *ADI* 7 (1981), págs. 201-223.

— (2019-2020), «La nueva Ley de Secretos empresariales», *ADI* 40 (2019-2020), págs. 141-164.

GURRY, Francis (2012) *Breach of Confidence*, Clarendon Press, Oxford.

HACKER, Philipp (2020), «Immaterialgüterrechtlicher Schutz von KI Trainingsdate», *GRUR* 10, págs. 1025-1033.

HARTMANN, Christian; ALLAN, Jacquelin E. M.; HUGENHOLTZ, P. Bernt; QUINTAIS, João P., y GERVAIS, Daniel (2020), «Trends and Developments in Artificial Intelligence Challenges to the Intellectual Property Rights Framework, Final report», Comisión Europea, págs. 1-178. Accesible en *https://op.europa.eu/en/publication-detail/-/publication/394345a1-2ecf-11eb-b27b-01aa75ed71a1/language-en*.

HILTY, Retro M.; HOFFMANN, Jörg, y SCHEUERER, Stefan (2020), «Intellectual Property Justification for AI», *Max Planck Institute for Innovation & Competition Research Paper No. 20-02*, págs. 1-29. Accesible en SSRN: *https://ssrn.com/abstract=3539406*.

HOFFMANN, Jörg, y OTERO, Begoña (2020), «Demystifying the role of data interoperability in the access and sharing debate», *JIPITEC* 11, pág. 252-273.

KERBER, Wolfgang (2016), «A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis», págs. 1-23. Accessible en SSRN: *https://ssrn.com/abstract=2858171*.

LEHR, David, y OHM, Paul (2017), «Playing with the Data: What Legal Scholars Should Learn about Machine Learning», *University of California, Davis, Law Review* 51, pág. 655-717.

LEISTNER, Matthias (2020), «The existing European IP rights system and the data economy - An overview with particular focus on data access and portability», págs. 1-44. Accesible en *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625712*.

LEMLEY M. A. (2008), «The Surprising Virtues of Treating Trade Secrets as IP Rights», *Stanford Law Review* 61, págs. 311 y sigs.

LOHSSE, Sebastian; SCHULZE, Reiner, y STAUDENMAYER, Dirk (2017), «Introduction», en LOHSSE, S.; REINER SCHULZE, R., y STAUDENMAYER, D. (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tool*s, Hart Publishing-Nomos, Germany, págs. 13-24.

MALGIERI, Gianclaudio (2016), «Trade Secrets v Personal Data: A possible solution for balancing rights», *International Data Privacy Law* 6, págs. 102-116.

MASSAGUER, José (1999), *Comentario a la Ley de Competencia Desleal,* Civitas, Madrid.

MATTIOLI, Michael (2018), «Autonomy in the Age of Autonomous Vehicles», *Boston University Journal of Science and Technology Law* 24, págs. 277-294.

METZGER, Axel (2020), «Access to and Porting of Data under Contract Law: Consumer Protection Rules and Market-Based Principles», págs. 1-19. Accesible en SSRN: *https://ssrn.com/abstract=3650301*.

NORDBERG, Ana (2020), «Trade Secrets, Big Data and Artificial Intelligence Innovation: A Legal Oxymoron?», en SCHOVSBO, J.; MINSSEN, T., y RIIS, T. (eds.), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive*, Edward Elgar Publishing, United Kingdom, págs. 192-219.

PASTOR, Eduardo (2020), «La acción de atribución en propiedad de mercancías infractoras de un secreto empresarial», *Diario La Ley*, núm. 9705, págs. 1-10.

PORTELLANO, Pedro (1997), «Protección de información no divulgada», en IGLESIAS, J. L. (dir.), *Los derechos de propiedad industrial en la organización Mundial del Comercio,* t. I, IDEI, Madrid, págs. 335-362.

PRICE II, W. Nicholson (2015), «Black-Box Medicine», *Harvard Journal of Law & Technology* 28 (2), págs. 420-467.

KATYAL, Sonia (2019), «Private Accountability in the Age of Artificial Intelligence», *UCLA L. Rev*. 66, págs. 54-141.

RUBINFELD, Daniel L., y GAL, Michal S. (2017), «Access Barriers to Big Data», *Arizona Law Review* 59, 2017, págs. 339-381.

SAGSTETTER, Thomas (2019), «Big Data und der europäische Rechtsrahmen: Status quo und Reformbedarf im Lichte der Trade-Secrets-Richtlinie 2016/943/EU», en MAUTE, L., y MACKENRODT, M. O. (eds.) *Recht als Infrastruktur für Innovation, Nomos Verlag, Nomos Verlag,* págs. 1-23. Accesible en SSRN: *https://ssrn.com/abstract=3219223*.

SAMUELSON, Pamela, y SCOTHMER, Suzanne (2002), «The Law and Economics of Reverse Engineering», *Yale L. J*. 111, págs. 1575-1662.

SAMUELSON, Pamela (2011), «First Amendment Defenses in Trade Secrecy Cases», en DREYFUSS, R. C., KATHERINE, J., y STRANDBURG, K. J. (eds.) *The Law and Theory of Trade Secrecy,* Edward Elgar Publishing Limited, Cheltenham UK, Northampton USA, págs. 269-299.

SCHEUERER, Stefan (2020), «Artificial Intelligence and Unfair Competition - Unveiling an Underestimated Building Block of the AI Regulation Landscape», *Max Planck Institute for Innovation & Competition Research Paper* No. 20-21, págs. 1-28. Accesible en SSRN: *https://ssrn.com/abstract=3744798 or http://dx.doi.org/10.2139/ssrn.3744798*.

SIMON, Brenda M., y SICHELMAN, Ted (2017), «*Data-Generating Patents*», *Northwestern University Law Review* 11, págs. 377-438.

STEPANOV, Ivan (2020) «Introducing a Property Right over Data in the EU: The Data Producer's Right - An Evaluation», *International Review of Law, Computers & Technology* 34, págs. 65-86.

SUÑOL, Áurea (2009), *El secreto empresarial. Un estudio sobre el artículo 13 de la Ley de competencia desleal*, Civitas-Thomson Reuters, Cizur Menor.

— (2019), «Big data, inteligencia artificial y secretos empresariales», *Almacén de Derecho*.

— (2020), «El Valor de un secreto empresarial», *Almacén de Derecho*.

SURBLYTĖ, Gintare (2016) «Data as Digital Resource», *Max Planck Institute for Innovation and Competition Research Paper No*. 16-12, págs. 1-40. Accesible en SSRN: *https://ssrn.com/abstract=2849303 or http://dx.doi.org/10.2139/ssrn.2849303*.

WIEBE, Andreas (2017), «Protection of industrial data - A new property right for the digital economy?», *JIPLP* 12, págs. 62-71.

ZECH, Herbert (2016), «A legal framework for a data economy in the European Digital Single Market: rights to use data», *Journal of Intellectual Property Law & Practice* 11, págs. 460-470.