

LA ADOPCIÓN DE MEDIDAS RAZONABLES PARA MANTENER SECRETA LA INFORMACIÓN COMO REQUISITO PARA LA EXISTENCIA DE UN SECRETO EMPRESARIAL

THE ADOPTION OF REASONABLE STEPS TO KEEP THE INFORMATION SECRET AS A REQUIREMENT FOR THE EXISTENCE OF A TRADE SECRET

RAFAEL GARCÍA PÉREZ*

RESUMEN

Según la Directiva sobre secretos empresariales, para que una información sea considerada secreto empresarial, la persona que legítimamente ejerza su control debe haber adoptado medidas razonables, en las circunstancias del caso, para mantenerla secreta (requisito de la adopción de medidas razonables). El presente artículo analiza este requisito, prestando especial atención a un aspecto que hasta el momento ha sido menos estudiado por la doctrina: ¿quién debe adoptar las medidas a las que se refiere el requisito?

Palabras clave: secretos empresariales, medidas razonables, competencia desleal, titular del secreto empresarial, poseedor del secreto empresarial.

ABSTRACT

According to the Trade Secrets Directive, for a piece of information to be considered a trade secret, it must have been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret (requirement of reasonable secrecy precautions). This article analyses the requirement, devoting special attention to one question that has been to some degree neglected so far: who must implement the precautions?

Keywords: trade secrets, reasonable precautions, unfair competition, trade secret owner, trade secret holder.

SUMARIO: I. PRELIMINAR.—II. ORIGEN HISTÓRICO DEL REQUISITO.—III. FUNCIONES.—IV. RELACIÓN CON LOS OTROS REQUISITOS QUE SE EXIGEN PARA LA EXISTENCIA DE

* Profesor Titular de Derecho Mercantil. Universidad de A Coruña. Dirección de correo electrónico: rafael.garcia.perez@udc.es.

UN SECRETO EMPRESARIAL.—V. REQUISITO OBJETIVO.—VI. EXIGENCIA DE UN COMPORTAMIENTO ACTIVO.—VII. REQUISITO DURADERO Y DINÁMICO.—VIII. MEDIDAS «RAZONABLES, EN LAS CIRCUNSTANCIAS DEL CASO».—1. Preliminar.—2. *Directiva vs. LSE*.—3. Apreciación de la razonabilidad.—4. Análisis funcional.—IX. TIPOS DE MEDIDAS.—X. ¿QUIÉN DEBE TOMAR LAS MEDIDAS?—1. Planteamiento del problema.—2. El debate en Alemania.—3. El debate en España.—4. Opinión del autor.—XI. BIBLIOGRAFÍA.

CONTENTS: I. INTRODUCTION.—II. THE HISTORICAL ORIGIN OF THE REQUIREMENT.—III. FUNCTIONS.—IV. RELATIONSHIP WITH THE OTHER REQUIREMENTS OF THE TRADE SECRET DEFINITION.—V. OBJECTIVE REQUIREMENT.—VI. REQUIREMENT OF ACTIVE BEHAVIOUR.—VII. PERSISTENT AND DYNAMIC REQUIREMENT.—VIII. «REASONABLE STEPS UNDER THE CIRCUMSTANCES».—1. Introduction.—2. *Directive vs. Trade Secrets Act*.—3. Assessment of the reasonableness of the steps taken.—4. Functional analysis.—IX. TYPES OF MEASURES.—X. WHO MUST ADOPT THE REASONABLE STEPS?—1. The problem.—2. The debate in Germany.—3. The debate in Spain.—4. Author's opinion.—XI. BIBLIOGRAPHY.

I. PRELIMINAR

La Directiva sobre secretos empresariales¹ establece una definición de «secreto comercial»² que incorpora la exigencia de que la información, además de ser secreta y tener un valor comercial por su carácter secreto, «ha[ya] sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control» (art. 2). La Ley española de secretos empresariales³ ha incorporado el requisito, si bien omite —de manera desafortunada— la referencia a «las circunstancias del caso». Según la Ley, se considera secreto empresarial cualquier información o conocimiento que, además de ser secreto y tener por ese motivo un valor empresarial real o potencial, «ha[ya] sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto» (art. 1).

En el presente estudio nos proponemos abordar el requisito. Pasaremos para ello casi por alto el tema que más ha tratado la doctrina —los tipos concretos de medidas que puede o debe adoptar el titular del secreto—, y nos centraremos en otros aspectos de interés que han sido menos estudiados.

II. ORIGEN HISTÓRICO DEL REQUISITO

Los orígenes del requisito se encuentran en el Derecho norteamericano. El origen remoto, según los estudios de Bone⁴, se remonta al momento en que los secretos empresariales se concebían como una forma de propiedad (siglo XIX)⁵.

¹ 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.

² La Directiva habla de «secretos comerciales», pero en adelante utilizaremos la expresión «secretos empresariales», que acuña en castellano el profesor GÓMEZ SEGADE en su clásica obra *El secreto industrial* (Know-how). *Concepto y protección* (1974, pág. 47), y que es la que emplea la Ley 1/2019, de 20 de febrero, de Secretos Empresariales (véase sobre esta opción del legislador el tercer párrafo del apartado III de la Exposición de Motivos).

³ Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

⁴ BONE (1998), págs. 251 y sigs., e *id.* (2011), págs. 49 y sigs.

⁵ En 1868, en el marco de una corriente jurisprudencial de «inmaterialización de la propiedad» (VANDELDE, 1980, págs. 333 y sigs.), los secretos empresariales se reconocen por primera vez en Estados Unidos como una forma de propiedad en el caso *Peabody vs. Norfolk*, 98 Mass. 452 (1868). En Inglaterra ya se había reconocido previamente este carácter en el caso *Morison vs. Moat* [9 Hare 241, 68 Eng. Rep. 492 (1851)]. *Vid.* VANDELDE (1980), págs. 351 y 352.

En el *common law*, para que existiese propiedad se exigía la posesión de la cosa: se requería que existiesen actos que manifestasen la intención del propietario de apropiarse la cosa y ejercer un control sobre la misma. Al concebirse el secreto empresarial como una forma de propiedad, se exigía la posesión del mismo. ¿Pero cómo se posee un bien inmaterial? En este caso por medio de la adopción de medidas razonables. En esta etapa remota, por tanto, y como consecuencia de esta concepción del secreto basada en la propiedad, «muchos tribunales empezaron a exigir, además del requisito de que la información fuese secreta, que se hubiesen adoptado precauciones razonables para mantenerla secreta, o al menos dudaban en considerar que la información era secreta cuando el demandante no había adoptado dichas precauciones»⁶.

La «teoría de la propiedad» fue perdiendo fuerza, en especial desde la Sentencia *Du Pont* del Tribunal Supremo⁷, con lo que el requisito de las medidas razonables pasó a un segundo plano. De hecho, en el *First Restatement of Torts* en 1939 la adopción de medidas pasa a ser simplemente uno de los seis factores relevantes para determinar si existe secreto. Ya no es un elemento imprescindible, pues, sino un factor más cuya ausencia puede ser compensada por los otros.

El requisito reaparecería, sin embargo, como elemento imprescindible para la existencia de secreto, en la *Uniform Trade Secrets Act* (en adelante, *UTSA*) de 1980, sin que se sepa muy bien el motivo. Bone ofrece la siguiente —poco satisfactoria— explicación: en el proyecto de la *UTSA* se exigía, como requisito para la tutela del secreto empresarial, que el mismo apareciese manifestado en forma tangible. El requisito fue eliminado, por lo que el mencionado autor conjetura que quizá la adopción de medidas se hubiese introducido para satisfacer un objetivo similar: identificar y fijar los límites de la información objeto de tutela⁸. Sea como fuere, la *UTSA* tuvo éxito, y de ella el requisito de las medidas razonables pasó al Acuerdo ADPIC (art. 39)⁹, y, por este cauce, desembocaría en la Directiva (art. 2)¹⁰.

III. FUNCIONES

Este epígrafe podría haberse titulado «fundamento» del requisito. Hablar de fundamentar, no obstante, implica la existencia de cierta racionalidad, de una construcción lógica a partir de unos cimientos. Sin embargo, y como hemos visto, el requisito de la adopción de medidas razonables tiene su origen remoto en peculiaridades del *common law* que no tienen razón de ser en nuestro ordenamiento, y su origen más próximo no tiene un fundamento claro. Por eso preferimos hablar de funciones del requisito, porque la expresión alude a determinados efectos que se desprenden del mismo, sin implicar que constituyan necesariamente su razón de ser.

⁶ BONE (1998), pág. 257.

⁷ *E. I. Du Pont De Nemours Powder Co. vs. Masland*, 244 U.S. 100, 102 (1917).

⁸ BONE (2011), pág. 57, n. 45. Sobre el aspecto de la tramitación de la *UTSA* al que hace referencia Bone, vid. SANDEEN (2010), pág. 525.

⁹ El Acuerdo ADPIC exige que la información «c) haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla».

¹⁰ «A los efectos de la presente Directiva se entenderá por:

1) «secreto comercial»: la información que reúna todos los requisitos siguientes: [...] c) haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control».

Una de las funciones que con mayor asiduidad invoca la doctrina¹¹ es la de advertencia o señalización: las medidas de tutela advierten a los terceros de que la información es confidencial. Dado el carácter inmaterial del secreto empresarial y las severas consecuencias aparejadas a una infracción, resulta necesario que los terceros sepan que determinada información es reservada. Las medidas razonables —por ejemplo identificar un documento como secreto, o el hecho de que esté en una caja fuerte o protegido por contraseña— advierten a los terceros de su carácter confidencial. Las medidas, en definitiva, desempeñan un papel similar al de la posesión con respecto de la propiedad, pero no en el sentido de constituir un requisito previo para su existencia (como hemos visto que sucedía en el *common law*), sino en el clásico de la función publicitaria de la posesión: esto tiene un dueño; hasta aquí lo mío¹². De hecho, para aquellos autores o tribunales que abordan el secreto desde el prisma del derecho de propiedad, y dada la naturaleza inmaterial del secreto, las medidas cumplen una función de demarcación del derecho de propiedad del titular¹³.

La segunda de las funciones del requisito está relacionada con la actitud diligente que debe mostrar quien ejercita un derecho. La necesidad de adoptar medidas razonables supone un acicate para la autotutela, o, dicho de otra forma, vigoriza la diligencia del poseedor de la información secreta y valiosa. De acuerdo con el clásico adagio «*vigilantibus non dormientibus iura succurrunt*», el Derecho tutelaré al poseedor diligente, que ha adoptado medidas para preservar el secreto, y no al descuidado o perezoso. Y es que como dice el juez Posner, si el actor ha invertido únicamente unos recursos ínfimos en evitar que la información caiga en manos de sus competidores, ¿por qué debería el Derecho, cuya maquinaria no es precisamente barata, molestarse en ampararlo?¹⁴ Lo que no se puede es ser dejado, aventurarse a que la información se filtre o divulgue, y pretender que los terceros estén obligados por aquello que uno mismo no respeta¹⁵. En definitiva, los tribunales no amparan al actor porque él mismo se la buscó («*he courted his own disaster*»), o porque no se merece otra cosa¹⁶.

La Directiva no parece ajena a esta función, pues en su propio Preámbulo indica que «se espera que el poseedor legítimo de un secreto comercial cumpla el deber de diligencia en lo que respecta al mantenimiento de la confidencialidad de su valioso secreto comercial y a la supervisión de su utilización»¹⁷.

¹¹ Por todos, SANDEEN (2014), págs. 42 y sigs.

¹² VARADARAJAN (2017) ha publicado un estudio en el que explica el requisito de la adopción de medidas razonables desde el punto de vista de la posesión. Afirma que: «*The primary purpose of the RSP requirement —like that of possession more broadly— is to notify a relevant audience about a proprietary claim*» (pág. 384).

¹³ El Tribunal Supremo norteamericano ha señalado que: «*Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others*». *Ruckelshaus vs. Monsanto Co.*, 467 U.S. 986, 1002 (1984). Las citas norteamericanas están tomadas de la base de datos *Westlaw Classic*, con el formato generado por la propia base.

¹⁴ *Rockwell Graphic Sys., Inc. vs. DEV Industries, Inc.*, 925 F.2d 174, 179 (7th Cir. 1991).

¹⁵ Parecido, «*I think one may not venture on liberties with his own secret, may not lightly or voluntarily hazard its leakage or escape, and at the same time hold others to be completely obligated to observe it*». *Gallowhur Chem. Corp. vs. Schwerdle*, 117 A.2d 416, 423 (N.J. Super. Ch. Div. 1955). A veces los tribunales han hecho referencia a la doctrina de las «*clean hands*», de fuerte arraigo en la *equity* [«*To put it another way, the employer must come into court with clean hands; the employer cannot complain of the employee's use of information if the employer has never treated the information as secret*». *Electro-Craft Corp. vs. Controlled Mot., Inc.*, 332 N.W.2d 890, 901 (Minn. 1983)].

¹⁶ *RTE Corp. vs. Coatings, Inc.*, 267 N.W.2d 226, 233 (Wis. 1978), con cita de CALLMANN (1968), sec. 55.1, págs. 451-53.

¹⁷ Considerando 23.

Quien no es diligente no merece el amparo legal, sobre todo en un ámbito que el legislador considera delicado, pues la Directiva ha establecido un sistema de frenos y contrapesos que trata de garantizar que la tutela del secreto empresarial no sea desproporcionada.

IV. RELACIÓN CON LOS OTROS REQUISITOS QUE SE EXIGEN PARA LA EXISTENCIA DE UN SECRETO EMPRESARIAL

Los distintos elementos configuradores de la definición de secreto empresarial (información secreta, valor empresarial y medidas razonables) tienen una relación entre sí, más o menos estrecha según los casos. Se aprecia claramente en el requisito del valor empresarial, que fluye de la exigencia de que la información sea secreta: el valor empresarial de la información o conocimiento deriva de «su carácter secreto» (Directiva) o existe «precisamente por ser secreto» (LSE).

En el caso de las medidas razonables, su existencia es un indicio del carácter secreto de la información, ya que, como ha destacado un tribunal norteamericano, «las medidas de seguridad, después de todo, cuestan dinero, por lo que un fabricante no incurriría en dichos costes si creyese que los competidores ya conocían la información en cuestión»¹⁸. La adopción de medidas, no obstante, no deja de ser un mero indicio, ya que por mucho que se fortifique una determinada información, lo que no es secreto no pasará a serlo. El carácter secreto, como ha apuntado el profesor Gómez Segade, es un requisito ontológico¹⁹, sin cuya concurrencia no puede existir el secreto empresarial. Lo ha apuntado otro de los grandes estudiosos del secreto empresarial, Milgrim, que afirma que aunque la existencia de medidas puede resultar un indicio de que la información es secreta, «*the most elaborative secrecy, however, will not elevate public knowledge to the status of a trade secret whereas the absence of sufficient precautions can forfeit secrecy*»²⁰.

Buena prueba de este aspecto es la sentencia norteamericana en el caso *Victor Chem. Works vs. Iliff*²¹, en la que se discutía si un procedimiento para la elaboración de fosfato de monocalcio constituía secreto empresarial. El Tribunal Supremo de Illinois considera que no lo tiene, ya que se trata de un proceso generalmente utilizado en la industria, incluso antes de que el actor comenzase a utilizarlo. En nada cambia la apreciación del Tribunal el hecho de que este adoptase medidas para proteger la información. Es cierto que fue muy cuidadoso: construyó altos muros, contrató personal de seguridad, restringió el acceso a sus instalaciones, exigió a sus químicos la firma de acuerdos de confidencialidad, etc. Todos estos elementos, concluye el Tribunal, pueden constituir un indicio de que existe un secreto empresarial, pero no son suficientes por sí mismos para determinar su existencia cuando la información, como en este caso, no es secreta. La demanda, en consecuencia, fue desestimada.

La adopción de medidas también es un indicio del valor empresarial del secreto, de manera que «cuanto más dinero gaste el titular en evitar que el secreto

¹⁸ *Metallurgical Industries Inc. vs. Fourtek, Inc.*, 790 F.2d 1195, 1199 (5th Cir. 1986).

¹⁹ GÓMEZ SEGADE (2019-2020), pág. 152.

²⁰ MILGRIM (2002), § 1.04, 1-175 (Rel.74-8/03 Pub. 738).

²¹ *Victor Chem. Works vs. Iliff*, 132 N.E. 806 (Ill. 1921).

se filtre, más demuestra que el secreto tiene un valor real merecedor de tutela jurídica»²². No obstante, de nuevo se trata de un mero indicio. Si la información no tiene valor empresarial, o su valor no deviene de su carácter secreto, de nada servirá construir altos muros. Estará protegida, pero carecerá del valor necesario para que nos encontremos ante un secreto empresarial.

V. REQUISITO OBJETIVO

La adopción de medidas razonables constituye un requisito de carácter objetivo²³. Con ello se quiere expresar que la mera voluntad de mantener oculta la información o de protegerla, o la convicción de que se trata de un secreto empresarial, no es suficiente. Lo verdaderamente relevante es que el poseedor haya adoptado las medidas y que estas sean razonables, desde el punto de vista de un observador imparcial, en las circunstancias del caso.

La Directiva opta, en este aspecto, por el modelo norteamericano, y rechaza el alemán.

En Alemania, antes de la entrada en vigor de la reciente Ley de tutela de los secretos empresariales no se exigía la adopción de *medidas razonables* para mantener la información secreta, sino la existencia de una *voluntad* de mantener la información secreta (*Geheimhaltungswille*)²⁴. Es cierto que la adopción de tales medidas era recomendable, pues de ella se deducía la existencia de la voluntad de mantener la información secreta, pero no resultaba imprescindible. Por regla general, la existencia de la *Geheimhaltungswille* se presumía, y la concurrencia del requisito no presentaba ningún problema de enjundia para el demandante²⁵.

En claro contraste con el modelo alemán, en el caso de la *UTSA* norteamericana lo determinante es la adopción de las medidas, no la voluntad del poseedor de la información, que por decidida que sea no puede suplir su ausencia. El problema se suscitó en el caso *Electro-Craft Corp. vs. Controlled Mot., Inc.*²⁶. El tribunal de primera instancia había apreciado que, aunque el demandante no había adoptado medidas de protección, sí había mostrado la voluntad de mantener sus datos y procesos secretos. El Tribunal Supremo de Minnesota considera

²² POSNER en *Rockwell Graphic Sys., Inc. vs. DEV Industries, Inc.*, 925 F.2d 174, 179-180 (7th Cir. 1991). Y a la inversa, «Failure to take such steps is persuasive evidence that the secret has no real value». *BondPro Corp. vs. Siemens Power Generation, Inc.*, 463 F.3d 702, 708 (7th Cir. 2006).

²³ *Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung*, https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_GeschGehG.pdf?__blob=publicationFile&vs.=1, comentario al § 2, pág. 24; TREBECK y SCHULTE-WISSERMANN (2018), pág. 1777; FERNÁNDEZ CARBALLO-CALERO (2013), pág. 415, y (2020), epígrafe 3 («Objeto de medidas razonables para mantener el secreto»); GÓMEZ SEGADÉ (2019-2020), pág. 154, y SANDEEN (2010), que señala que: «Wishful thinking is not enough. Rather, only information that is actually subject to reasonable secrecy efforts meets the definition of a trade secret» (pág. 527).

²⁴ La nueva Ley (*Gesetz zum Schutz von Geschäftsgeheimnissen* de 18 de abril de 2019) prescinde del requisito de la *Geheimhaltungswille*. Curiosamente, incorpora un requisito que la Directiva solo menciona en el Preámbulo (cdo. 14): debe existir un interés legítimo en el mantenimiento de la confidencialidad de la información [§ 2.1.c)].

²⁵ HOEREN (2021), § 2 *Begriffsbestimmungen*; KÖHLER (2018), *UWG* § 17 apdo. 10; KALBFUS (2016), pág. 1011, y OHLY (2014), págs. 4 y 5, este último muy crítico con el requisito, que en su opinión era innecesario y engañoso. Debe precisarse que la mera voluntad no era, no obstante suficiente, ya que se exigía la existencia de un interés objetivo en la existencia del secreto. *Vid.* KALBFUS (2017B), *UWG* § 17, apdo. 1-6.1.

²⁶ *Electro-Craft Corp. vs. Controlled Mot., Inc.*, 332 N.W.2d 890, 901 (Minn. 1983).

que la mera voluntad es irrelevante para determinar si se satisface el requisito de la adopción de medidas razonables. Afirma que la referencia que el tribunal de instancia hace a la voluntad hunde sus raíces en el test del *common law* para determinar la existencia de secreto (y no en la *UTSA*, por tanto). Y es más, apunta que incluso bajo el *common law*, se requería más que la mera voluntad; el actor debía mostrar que había manifestado dicha voluntad haciendo algún esfuerzo para mantener la información secreta.

VI. EXIGENCIA DE UN COMPORTAMIENTO ACTIVO

El hecho de que la Directiva introduzca el requisito de la adopción de medidas razonables implica que el hecho de que la información sea valiosa y se mantenga, de hecho, secreta, no es suficiente para que exista un secreto empresarial. Es necesario, por el contrario, que el poseedor de la información adopte medidas *de forma activa* para mantener el secreto²⁷. La inacción se castiga, y no es excusa el argumento de que se consideraba que la mejor forma de no despertar el interés de terceros era no adoptar medida alguna²⁸. Es decir, no es posible alegar que la *no actuación* es una medida. El argumento de que no se actuó porque esa era la mejor forma de asegurar la confidencialidad de la información está condenado al fracaso.

VII. REQUISITO DURADERO Y DINÁMICO

El requisito de la adopción de medidas razonables impone una carga que se prolonga en el tiempo²⁹. Es decir, no se exige únicamente en un momento inicial, para que nazca la protección, sino que debe mantenerse³⁰ («*One who claims a trade secret must exercise eternal vigilance in protecting its confidentiality*»; *RTE Corp. vs. Coatings, Inc.*³¹). Ahora bien, puede no ser suficiente con mantener las mismas medidas de protección durante toda la vida del secreto, puesto que la Directiva impone que la información haya sido objeto de medidas razonables, *en las circunstancias del caso*, para mantenerla secreta. El hecho de que las medidas deban ser razonables *en las circunstancias del caso* implica lógicamente que, si varían las circunstancias, las medidas deban adaptarse. Por eso se ha podido afirmar que se trata de un requisito *dinámico*³².

Además, el hecho de que la carga se prolongue en el tiempo conlleva una importante consecuencia: la persona obligada a adoptar las medidas razonables puede cambiar, a medida que el control legítimo sobre el secreto se desplace

²⁷ TREBECK y SCHULTE-WISSERMANN (2018), pág. 1777, e *Incase, Inc. vs. Timex Corp.*, 488 F.3d 46, 53 (1st Cir. 2007) («*there must be affirmative steps to preserve the secrecy of the information as against the party against whom the misappropriation claim is made*»).

²⁸ *J. T. Healy & Son, Inc. vs. James A. Murphy & Son, Inc.*, 260 N.E.2d 723, 730 (Mass. 1970).

²⁹ HAUCK (2019), pág. 225.

³⁰ El propio término *mantenerse*, que es el que emplea la Directiva («medidas razonables, en las circunstancias del caso, para mantenerla secreta»), es expresivo de este carácter duradero o sostenido en el tiempo.

³¹ *RTE Corp. vs. Coatings, Inc.*, 267 N.W.2d 226, 233 (Wis. 1978).

³² LEISTER (2019), pág. 76. Este carácter dinámico impone que el poseedor del secreto mantenga una actitud vigilante, y monitorice y evalúe de forma regular la situación para adoptar las medidas que pudieran resultar necesarias en las nuevas circunstancias. SLABY, CHAPMAN y O'HARA (1989), pág. 325. La vigilancia debe extremarse en especial en el aspecto informático, ya que los cambios vertiginosos en este ámbito pueden hacer que las medidas queden rápidamente desfasadas. CUNDIFF (2009), págs. 359 y sigs.

de unas personas a otras. Si el secreto se cede, por ejemplo, el cesionario será el nuevo poseedor y, como tal, el obligado a adoptar las medidas razonables. Y si se concede una licencia que otorga el control al licenciario, este deberá adoptar también medidas razonables. Trataremos este aspecto con mayor detenimiento en el último epígrafe de este trabajo.

VIII. MEDIDAS «RAZONABLES, EN LAS CIRCUNSTANCIAS DEL CASO»

1. Preliminar

La Directiva establece que la información debe «haber sido objeto de medidas *razonables, en las circunstancias del caso*, para mantenerla secreta». El inciso entrecomillado introduce un punto de medida en el requisito, pues proscribire una interpretación excesivamente severa y rígida del mismo. Esta medida es coherente con los objetivos de la Directiva³³. El considerando 9 de su Preámbulo considera que uno de los aspectos que justifican la promulgación de la Directiva consiste en evitar que la insuficiente tutela jurídica en algunos Estados miembros provoque una asignación de capital ineficiente (los poseedores de secretos invertirían en medidas de protección, en lugar de hacerlo en actividades innovadoras). Pues bien, si uno de los objetivos de la Directiva es evitar un gasto desproporcionado en la protección del secreto, contravendría el objetivo exigir medidas desproporcionadas para mantener la información secreta. Lo que se exige es que se adopten medidas razonables, no las mejores o más eficaces que se puedan concebir³⁴. A esto se refería el juez Posner cuando aseguró que «[s]i los secretos empresariales se protegen únicamente en el caso de que sus titulares adopten, para mantener su secreto, medidas extravagantes que perjudican la productividad, se reducirá el incentivo para invertir recursos en el descubrimiento de métodos de producción más eficientes y, con ello, la innovación»³⁵.

Seguidamente expondremos la manera en la que ha de apreciarse la concurrencia del requisito, a la luz de la exigencia de que se haga de forma mesurada e individualizada. Pero antes repararemos en un punto criticable de la LSE: la omisión del inciso de la Directiva que alude a «las circunstancias del caso».

2. *Directiva vs. LSE*

La Directiva establece que la información debe «haber sido objeto de *medidas razonables, en las circunstancias del caso*, para mantenerla secreta» (énfasis añadido). La LSE prescinde del inciso «en las circunstancias del caso», pese a que el Informe del CGPJ había criticado la omisión en el Anteproyecto³⁶. En Alemania sucedió algo similar. El Proyecto del Gobierno omitía la referencia a las circunstancias del caso, pero allí las críticas sí fueron es-

³³ KALBFUS (2017A), pág. 392.

³⁴ *Ibid.*

³⁵ *Rockwell Graphic Sys., Inc. vs. DEV Industries, Inc.*, 925 F.2d 174, 180 (7th Cir. 1991).

³⁶ «Informe sobre el Anteproyecto de Ley de Secretos Empresariales», apdo. 56, pág. 20. Disponible en <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Actividad-del-CGPJ/Informes/Informe-sobre-el-Anteproyecto-de-Ley-de-Secretos-Empresariales>.

cuchadas y el legislador fue fiel al texto de la Directiva en el texto finalmente promulgado³⁷.

La omisión, pese a que no tiene verdadera relevancia a efectos prácticos, ya que las circunstancias del caso han de valorarse como resultado de una interpretación conforme, es desafortunada. Y es que aunque es cierto que un juicio de razonabilidad no puede hacerse nunca en el vacío, sino que debe siempre estarse a las circunstancias concretas que rodean el supuesto de hecho, lo cierto es que el aserto ofrece una guía al Tribunal para la concreción de la razonabilidad. Su omisión podría llevar a una aplicación descuidada que no tuviese en cuenta las peculiaridades del caso concreto³⁸.

3. Apreciación de la razonabilidad

El requisito —de carácter objetivo, como sabemos— exige que se hayan adoptado «medidas razonables, en las circunstancias del caso». Es decir, que se requiere una valoración objetiva, que tenga en cuenta las particularidades del caso enjuiciado, sobre la razonabilidad de las medidas adoptadas. O formulado en forma de pregunta: ¿consideraría un observador imparcial, a la vista de las particularidades que rodean el caso, que las medidas que se han adoptado son razonables?³⁹. En este análisis se pueden diferenciar tres elementos:

a. El observador imparcial

El análisis debe hacerse desde un punto de vista objetivo, sin que sea relevante la intención del poseedor de la información. No importa que tuviese una decidida voluntad de mantenerla secreta o de protegerla, o que la considerase confidencial o valiosísima. Lo relevante son las medidas que haya adoptado.

b. La razonabilidad

Como hemos dicho, la razonabilidad introduce un elemento de medida en el requisito de la adopción de medidas para mantener secreta la información. No se requiere adoptar medidas heroicas⁴⁰, ni extravagantes⁴¹, ni extremas⁴². Tampoco es necesario realizar todos los esfuerzos posibles⁴³, y ni siquiera se exige que las medidas sean las óptimas⁴⁴, pues lo razonable no tiene por qué coincidir con lo óptimo, del mismo modo que se dice que lo mejor es enemigo de lo bueno. En definitiva, no es necesario que se construya una fortaleza in-

³⁷ MAAßEN (2019), pág. 353. Vid. las críticas del Max Planck (https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Stellungnahme_zum_Referentenentwurf_eines_Gesetzes_zur_Umsetzung_der_Richtlinie_EU_2016_943.pdf) y de la GRUR (WÜRTEMBERGER y FREISCHMIDT (2018), pág. 709).

³⁸ Vid. las consideraciones críticas que realiza el profesor GÓMEZ SEGADÉ (2019-2020), págs. 154 y 155. También se muestra crítica SUNOL LUCEA (2020-2021), pág. 201).

³⁹ ALEXANDER (2022, *GeschGehG* § 2, apdo. 66) propone, de manera sensata, tener en cuenta el punto de vista de un observador objetivo y perspicaz del círculo de personas (especializadas) que usualmente tratan con este tipo de información.

⁴⁰ «We do not require the possessor of a trade secret to take heroic measures to preserve its secrecy», *USM Corp. vs. Marson Fastener Corp.*, 393 N.E.2d 895, 902 (Mass. 1979).

⁴¹ «The owner of the secret must take reasonable, though not extravagant, measures to protect its secrecy». *Flotec, Inc. vs. S. Research, Inc.*, 16 F. Supp. 2d 992, 1000 (S.D. Ind. 1998).

⁴² DOLE (2016), pág. 102.

⁴³ «Only reasonable efforts, not all conceivable efforts, are required to protect the confidentiality of putative trade secrets», *Surgidev Corp. vs. Eye Tech., Inc.*, 828 F.2d 452, 455 (8th Cir. 1987).

⁴⁴ MAAßEN (2019), pág. 353, con ulteriores citas. Se trata de que se adopten medidas razonables, no las mejores medidas posibles. KALBFUS (2017A), pág. 392.

expugnable⁴⁵. Erraría por tanto el tribunal que exagerase su celo e impusiese exigencias desproporcionadas⁴⁶.

Por otro lado, las medidas pueden ser consideradas razonables aunque hayan fracasado, pues otra cosa nos conduciría al absurdo de negar la tutela en todo caso, ya que si se ejercitan acciones es porque las medidas fallaron. Basta con que, consideradas *ex ante*, las medidas sean razonables⁴⁷. Como ha indicado un tribunal norteamericano, «[e]n tanto que las precauciones tomadas hayan sido razonables, no importa que el demandado haya encontrado una manera de eludirlas»⁴⁸.

c. Las circunstancias del caso

La apreciación de la razonabilidad debe realizarse de manera individualizada, ya que unas medidas que podrían resultar razonables en un contexto fáctico podrían no serlo en otro. La Directiva no ofrece guía, no obstante, a este respecto, y no existe una enumeración, siquiera a modo de lista abierta, de las circunstancias a tener en cuenta. Sí existen, sin embargo, algunos factores que la jurisprudencia y doctrina han considerado especialmente relevantes, y que mencionamos a continuación.

Uno de los aspectos fundamentales a tener en cuenta para determinar si las medidas son razonables es el del valor de la información. No resultaría proporcionado exigir las mismas medidas protectoras para un secreto empresarial de extraordinaria importancia para la empresa que para un secreto menor. De hecho, alguna doctrina distingue, en función del perjuicio supondría que el secreto se divulgase, entre tres tipos de secretos. En primer lugar, se encontrarían las «joyas de la corona», cuya divulgación podría poner en peligro la propia existencia de la empresa. En segundo lugar, la «información importante», cuya revelación podría causar un perjuicio económico duradero. Por último, se encuentra la «información sensible», cuyo conocimiento podría causar un perjuicio económico transitorio⁴⁹. No existe una cuarta categoría de información poco relevante, ya que, como dispone la Directiva en su Preámbulo, «[s]e excluye de la definición de secreto comercial la información de escasa importancia»⁵⁰.

La clasificación de los secretos no es estrictamente necesaria, pero puede ser una herramienta útil para valorar el caso concreto. Y es que cuanto más importante sea la información, mayores medidas habrá que adoptar para alcanzar el objetivo de la «razonabilidad». No sería razonable, por ejemplo, que las medidas para proteger un secreto de gran importancia descrito en un documento se limitasen a señalar en su primera página que se trata de «información confidencial»⁵¹. Lo paradójico a este respecto es que describir en la demanda el

⁴⁵ «Reasonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement, and we are not disposed to burden industrial inventors with such a duty in order to protect the fruits of their efforts». *E. I. duPont de Nemours & Co. vs. Christopher*, 431 F.2d 1012, 1017 (5th Cir. 1970).

⁴⁶ THIEL (2019), pág. 701, con ulteriores citas.

⁴⁷ MCGUIRE (2019), pág. 2216.

⁴⁸ «So long as the precautions taken were reasonable, it doesn't matter that the defendant found a way to circumvent them». *Compulife Software Inc. vs. Newman*, 959 F.3d 1288, 1312 (11th Cir. 2020). Puede ayudar la analogía con las obligaciones de medios y de resultado. Como señala TRALLERO OCAÑA (2021, pág. 315), «courts should be mindful that the obligation concerns the means, not the outcome».

⁴⁹ MAAßEN (2019), pág. 356, con ulteriores referencias.

⁵⁰ Considerando 14.

⁵¹ LEISTER (2019), pág. 76.

secreto como especialmente valioso y trascendental para la empresa —exagerar en la demanda, lo cual puede parecer muy natural— puede volverse en contra del actor, ya que el nivel de exigencia para alcanzar la «razonabilidad» será mayor⁵².

Otro de los aspectos destacados para determinar si las medidas son razonables es el de las características de la empresa en cuestión. No se pueden exigir las mismas medidas a una gran empresa que a una pequeña o mediana empresa⁵³. En estrecha relación con lo anterior, la capacidad financiera también resulta relevante, ya que de una empresa con mayores recursos pueden esperarse medidas más estrictas. Por el contrario, no sería proporcionado exigir a una empresa en dificultades económicas instalar un complejo y caro sistema de seguridad que pudiese poner en peligro su estabilidad financiera⁵⁴.

Por último, también puede ser relevante el sector en el que se incardina la empresa. En los sectores muy competitivos en los que la información desempeña un papel fundamental, parece razonable exigir la adopción de medidas más rigurosas que en otros sectores que no reúnen esas características⁵⁵. Y si en un sector el espionaje industrial es frecuente, resulta lógico que se exija al poseedor de la información estar más alerta y reforzar sus medidas de seguridad que si se trata de un sector donde el espionaje constituye una rareza⁵⁶.

4. Análisis funcional

Reparar en las funciones que desempeña el requisito de la adopción de medidas para mantener la información secreta puede ayudar a realizar una apreciación sensata de la razonabilidad. Recordemos que las principales funciones del requisito son la de fomentar el comportamiento diligente del poseedor de la información, y la de advertir a los terceros de que se encuentran en presencia de información confidencial. Ambas funciones pueden servir para juzgar si las medidas adoptadas son razonables. Serán razonables las medidas, en este sentido, que demuestren que el poseedor de la información no ha sido negligente, sino que ha actuado con un nivel de diligencia medio; es decir, que muestren que ha sido vigilante, precavido, prudente. Por el contrario, las medidas no serán razonables cuando muestren dejadez, desidia o abandono por parte del poseedor de la información. Es curioso, a este respecto, que el *DRAE* define «medida», en una de sus acepciones, como «prevención»⁵⁷, y que la versión portuguesa habla

⁵² En la Sentencia de la AP de Barcelona de 17 de diciembre de 2019, por ejemplo, se destaca que «la expresión legal se refiere a «medidas razonables» de protección de la información secreta, según dicción del artículo 39.2 ADPIC, medidas que en este caso calificamos como ordinarias, insuficientes para conseguir una adecuada protección de los datos que se querían proteger, ante la especial importancia que la actora atribuye a la información descrita como secreto». SAP de Barcelona, Secc. 15.ª, de 17 de diciembre de 2019, ECLI:ES:APB:2019:15599 (aplica la LCD). Énfasis añadido.

⁵³ *Learning Curve Toys, Inc. vs. Playwood Toys*, 342 F.3d 714, 724 (7th Cir. 2003).

⁵⁴ SLABY, CHAPMAN y O'HARA (1989), pág. 334.

⁵⁵ *Ibid.*, pág. 333.

⁵⁶ *Ibid.*, y *Electro-Craft Corp. vs. Controlled Mot., Inc.*, 332 N.W.2d 890, 902 (Minn. 1983).

⁵⁷ «6. f. Disposición, prevención. U. m. en pl. Tomar, adoptar medidas». <https://dle.rae.es/medida>. También la palabra utilizada en la versión italiana, «misura», tiene la acepción de «d. *Precauzione, provvedimento preso per conseguire un fine e soprattutto per garantirsi da un male, da un danno: ho agito così per una semplice m. di prudenza. Per lo più al plur. (per imitazione dell'uso francese): non mi fido di lui, e prima di accettare la sua proposta voglio prendere le mie m.; prendere m. energiche per evitare disordini; stabilire m. preventive, restrittive, ecc.*» <https://www.treccani.it/vocabolario/misura/>.

de «diligências [razoáveis]», palabra que en una de sus acepciones significa «*Aplicação, zelo, cuidado* (para conseguir algo)»⁵⁸.

En segundo lugar, puede resultar útil, a la hora de determinar la razonabilidad, indagar si las medidas eran suficientes para advertir a los terceros de que se encontraban en presencia de información confidencial⁵⁹. Si los terceros no tenían forma de saber que la información era secreta, lo más probable es que sea debido a que no se han adoptado medidas razonables para mantener ese estatus secreto de la información.

En definitiva, puede ser útil hacerse dos preguntas: *a)* ¿Las medidas adoptadas por el poseedor de la información muestran que ha actuado con diligencia media, o más bien ponen de manifiesto su desidia o abandono?; y *b)* ¿Las medidas adoptadas, permitían a los terceros advertir que se estaban relacionando con información reservada, o más bien los terceros no estaban en condiciones de advertir que se encontraban ante una información de este tipo?

Debe tenerse, en cuenta, no obstante, que las anteriores preguntas constituyen una mera herramienta metodológica dirigida a evitar descontextualizar el requisito e impedir una aplicación irreflexiva del mismo. Son herramientas para pensar el requisito, no preguntas que haya que contestar afirmativamente en todo caso antes de concluir que nos encontramos ante un secreto empresarial.

IX. TIPOS DE MEDIDAS

Ya hemos señalado que el objetivo de este trabajo no es tratar del tipo de medidas a adoptar, aspecto muy estudiado por la doctrina⁶⁰. Sí que es importante, no obstante, recalcar la conveniencia de que la adopción de medidas esté encuadrada en una estrategia global de gestión de los secretos de la empresa y la necesidad de que las medidas sean específicas.

a. Estrategia global: la tutela de los secretos no debe concebirse como la simple puesta en marcha de determinadas medidas protectoras (por ejemplo guardar un documento en una caja fuerte en una estancia a la que solo se pueda acceder con un código), sino que dichas medidas protectoras deben concebirse como parte de una estrategia general de protección del secreto. Por este motivo, las contribuciones doctrinales más interesantes son las que exponen una estrategia en varias fases, más que las que enumeran sin más determinadas medidas a adoptar⁶¹. Además, el contar con esta estrategia demuestra la diligencia del titular; es decir, la propia estrategia es una «medida razonable» en el sentido de la Directiva. En este sentido el empleo en la versión española de la palabra «medida» conlleva el peligro de adoptar una visión limitada e individualizada, en lugar de un enfoque global de los esfuerzos de protección adoptados por el poseedor. De hecho, la versión inglesa de la Directiva habla de «*reasonable steps*», y la *UTSA* de «*efforts that are reasonable*», lenguaje que carece de la connotación individualista de la versión española. Debe evitarse, por tanto, una

⁵⁸ «*Diligência*», en el Dicionário Priberam da Língua Portuguesa [em linha], 2008-2021, <https://dicionario.priberam.org/dilig%C3%A2ncia>.

⁵⁹ Sobre este aspecto, *vid.* SUNOL LUCEA (2009), págs. 175 y sigs. y 185 y sigs.

⁶⁰ Por todos, *ibid.*, págs. 156 y sigs.

⁶¹ Aunque estas últimas pueden ser muy útiles. *Vid.*, por ejemplo, la lista del artículo de NEALEY, DAIGNAULT y CAI (2015).

apreciación aislada o individualizada de las medidas, o limitarse simplemente a escoger algunas para cubrir el expediente. Lo fundamental es que, apreciadas en su conjunto, las medidas proporcionen una protección adecuada y eficaz. Se trata, en fin, de una estructura, de un sistema integrado de tutela, por lo que ha de prestarse atención al resultado final que arrojan las diferentes medidas adoptadas⁶².

Una de las propuestas de estrategia propone que en una primera fase se identifiquen los secretos, se clasifiquen (por ejemplo según su importancia para la empresa) y se determinen los potenciales riesgos de que los mismos se filtren. En una segunda fase, se diseñaría y ejecutaría un plan de protección que incluyese medidas organizativas, técnicas y jurídicas. Una última fase comprendería la comprobación periódica de la efectividad de las medidas y, en su caso, su puesta al día⁶³. Otra propuesta incluye una primera etapa consagrada a identificar las personas o equipos que son responsables de los diferentes secretos⁶⁴, y una tercera propuesta dedica una segunda fase, después de una primera destinada a identificar los secretos empresariales, a etiquetarlos o marcarlos como confidenciales.

b. Medidas específicas: las medidas deben estar dirigidas a la tutela del concreto secreto empresarial que se invoca. Las medidas de seguridad generales no son suficientes. Se observa bien en un caso resuelto por el décimo circuito⁶⁵. El Tribunal de instancia, que se había decantado por considerar que la información relativa a los precios de la actora constituía un secreto empresarial, había puesto especial énfasis en las medidas adoptadas por el demandante: los empleados firmaban acuerdos de confidencialidad, se usaban contraseñas para restringir el acceso a la información confidencial de la empresa, se recordaba con frecuencia a los empleados que la información de la empresa tenía carácter reservado, y la empresa había gastado a lo largo de sus treinta años de historia cientos de miles de dólares en reunir la información y mantener su confidencialidad. En el recurso, el décimo circuito, por el contrario, consideró que no existía secreto empresarial: los anteriores hechos prueban que el demandante adopta «medidas *generales* para mantener la información reservada»⁶⁶. Sin embargo, ello no sucedía en lo que a la información relativa a los precios se refiere, y esta era precisamente la información que el actor consideraba secreta⁶⁷.

La especificidad de las medidas cobra especial importancia en relación con los acuerdos de confidencialidad. Al respecto, se desaconsejan aquellos acuer-

⁶² ALEXANDER (2022), *GeschGehG* § 2, apdo. 54.

⁶³ LEISTER (2019), pág. 77.

⁶⁴ TREBECK y SCHULTE-WISSERMANN (2018), pág. 1778.

⁶⁵ *S.W. Stainless, LP vs. Sappington*, 582 F.3d 1176 (10th Cir. 2009).

⁶⁶ Cursiva en el original.

⁶⁷ En la jurisprudencia española, *vid.* SAP Madrid, Secc. 28.ª, de 26 de abril de 2019, ECLI:ES:APM:2019:13399: «No basta como tal decir que el ordenador de cada empleado tenía un nombre de usuario y clave (es lógico en todos los puestos de trabajo informáticos) o que el demandado había firmado en 2011 un “Documento de Seguridad para la Protección de Datos de carácter personal de Maquinaria Conservera Tomas Guillen SL”, que se limita a establecer obligaciones de orden general sobre el uso de ficheros, materiales, recursos, ordenadores portátiles, terminales de trabajo, etc. , pero que no contiene medidas técnicas concretas de salvaguarda de la información de valor empresarial de la actora» (se aplica la LCD). *Vid.*, también, SAP Barcelona, Secc. 15.ª, de 14 de octubre de 2010, ECLI:ES:APB:2010:11709: «el artículo 39.2 ADPIC [...] no se refiere a los simples controles de seguridad ordinarios en la gestión de los datos de cualquier empresa, sino a medidas extraordinarias, que resulten especialmente indicativas del carácter secreto de la información que con ellas se quiere preservar».

dos que imponen obligaciones generales. Es preferible una regulación más específica que concrete el contenido y límites de la obligación de reserva⁶⁸. El *Landesarbeitsgericht Düsseldorf*, por ejemplo, tuvo por insuficiente una cláusula del contrato de trabajo que obligaba a mantener la confidencialidad al trabajador. Estimó que la cláusula era tan amplia e indeterminada que, de considerarla suficiente, estaría vaciando de contenido el requisito legal de la adopción de medidas razonables para mantener la información secreta⁶⁹.

X. ¿QUIÉN DEBE TOMAR LAS MEDIDAS?

1. Planteamiento del problema

La Directiva, cuando proporciona una definición de secreto empresarial, establece que las medidas razonables han de ser «tomadas por la persona que legítimamente ejerza su control» (art. 2). Se plantea, en consecuencia, la necesidad de precisar quién es esa persona (o personas) que ejerce legítimamente el control. El resultado al que lleguemos no es puramente teórico, sino que puede ser de importancia capital en un litigio, ya que si por ejemplo consideramos que el licenciatario ejerce el control legítimo, entonces no habrá secreto si las medidas las ha adoptado únicamente el titular⁷⁰.

La respuesta a bote pronto podría ser que quien debe tomar las medidas es el poseedor del secreto, ya que la propia Directiva define al «poseedor de un secreto comercial» como «cualquier persona física o jurídica que legítimamente ejerza el control de un secreto comercial» (art. 2). No obstante, este razonamiento no es plenamente satisfactorio, ya que estamos introduciendo el concepto definido en la definición: *secreto empresarial* es la información secreta y valiosa con respecto a la cual el poseedor del *secreto empresarial* ha adoptado medidas. Para evitar esta incorrección, la Directiva — más depurada técnicamente en este punto que la LSE—⁷¹ impone la carga a quien ejerce legítimamente el control de la información (no del secreto), como se aprecia con especial claridad en la versión inglesa («*it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret*»). Nada raro tiene esta forma de proceder ya que la definición, al fin y al cabo, describe las condiciones necesarias para que exista un secreto empresarial, por lo que la adopción de medidas es un *prius* con respecto a la existencia del secreto. No hay poseedor del secreto empresarial antes de que este nazca⁷².

En definitiva, en un primer momento, las medidas las adopta quien ejerce el control sobre la información, y si esta además es secreta y tiene valor empresarial por el hecho de ser secreta, entonces, al adoptar las medidas, surge un secreto empresarial (en sentido jurídico) y un poseedor del secreto empresarial

⁶⁸ ALEXANDER (2017), pág. 1039.

⁶⁹ *Landesarbeitsgericht Düsseldorf*, Sentencia de 3 de junio de 2020, 12 SaGa 4/20, apdo. 116.

⁷⁰ RABASA MARTÍNEZ (2018), nota 25.

⁷¹ La Ley española hace referencia a la adopción de medidas razonables por parte de su «titular», cuando en realidad hasta que se adoptan las medidas no se es titular del secreto en sentido jurídico, pues este no ha adquirido tal condición (jurídica de secreto empresarial).

⁷² No puede argumentarse que poseedor es quien adopta las medidas. Si una persona no ejerce el control de la información, por muchas medidas que adopte no nacerá el secreto empresarial y no será, por tanto, poseedor del mismo (pues no existe). Y si el secreto empresarial existe, pero no ejerce el control, tampoco será poseedor del mismo aunque adopte medidas para protegerlo.

(también en sentido jurídico). Desde ese momento, en que ya existe el secreto empresarial, ya se puede decir con propiedad que la carga recae sobre el poseedor (o poseedores) del secreto⁷³. Además, al ser la carga de adoptar medidas de carácter duradero, si el poseedor cambia, la carga recae sobre el nuevo poseedor.

Más allá de esta precisión de técnica jurídica, la diferencia no tiene mayor trascendencia, ya que no existe ningún motivo para pensar que la Directiva haya querido diferenciar entre los conceptos de control legítimo *de la información* y control legítimo *del secreto empresarial* («*ubi lex non distinguit, nec nos distinguere debemus*»). En realidad, en este último caso se trata también de ejercer el control legítimo sobre una información, pero sobre una información cualificada, porque reúne una serie de condiciones (es secreta, tiene valor empresarial y se han adoptado medidas razonables para mantenerla secreta).

Como quiera, por tanto, que la diferenciación no tiene mayor relevancia jurídica, podremos valernos de la abundante doctrina que analiza el significado de poseedor del secreto para tratar de esclarecer qué significa ejercer el control legítimo. Una vez hecho esto, estaremos en condiciones de precisar quién es la persona que debe adoptar las medidas razonables para mantener la información secreta.

Comenzaremos, pues, por exponer el debate doctrinal en torno al concepto de poseedor del secreto empresarial, y luego ofreceremos nuestra postura al respecto y las implicaciones que tiene con respecto al tema que nos ocupa.

2. El debate en Alemania

En Alemania existe un vivo debate en torno al significado del término «poseedor del secreto empresarial». Se discute especialmente si el licenciatario es poseedor del secreto. La tramitación de la Ley alemana se muestra favorable a incluir al licenciatario entre los poseedores. No solo el Proyecto del Gobierno afirma expresamente en su explicación que el licenciatario puede encajar en el concepto de poseedor⁷⁴, sino que incluso la definición original del Proyecto de Ley fue modificada precisamente porque podía dejar de lado a los licenciatarios.

Según la definición del Proyecto, en efecto, el poseedor del secreto era cualquier persona natural o jurídica que haya obtenido legítimamente un secreto empresarial y que pueda utilizarlo y revelarlo⁷⁵. En su opinión sobre el Proyecto, tanto el Instituto Max Planck⁷⁶ como la *Deutsche Vereinigung für Gewerblichen Rechtsschutz und Urheberrecht e. V. (GRUR)*⁷⁷ consideraron que la definición era desafortunada, ya que podía excluir al licenciatario, puesto que normalmente el contrato de licencia impone limitaciones al uso del secreto e

⁷³ Si procedemos a la integración de la definición de secreto en la definición de poseedor de un secreto empresarial nos encontramos con el siguiente resultado: «poseedor de un secreto comercial» es cualquier persona física o jurídica que legítimamente ejerza el control de una información que sea secreta, tenga por ello un valor comercial y haya sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control (es decir, por ella, por el poseedor).

⁷⁴ Citado *supra*, comentario al § 2, pág. 23.

⁷⁵ «*Jede natürliche oder juristische Person, die ein Geschäftsgeheimnis rechtmäßig erlangt hat und das Geschäftsgeheimnis nutzen und offenlegen darf*».

⁷⁶ https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Stellungnahme_zum_Referententwurf_eines_Gesetzes_zur_Umsetzung_der_Richtlinie_EU_2016_943.pdf.

⁷⁷ WÜRTENBERGER y FREISCHEM (2018).

impide su revelación. La *GRUR* consideraba que dejar al margen al licenciataria sería contrario a la Directiva, por lo que se aconsejaba optar por una definición más fiel a su tenor literal⁷⁸, y el *Max Planck* estimaba que la definición creaba una innecesaria inseguridad⁷⁹. La versión final de la Ley se doblegó a la crítica, y calcó casi palabra por palabra la definición de la Directiva⁸⁰.

Con estos precedentes es natural que buena parte de los autores alemanes se inclinen por considerar que el licenciataria es o puede ser poseedor del secreto⁸¹. No obstante, existen autores con posturas contrarias o bien intermedias. McGuire, que expresa abiertamente sus dudas sobre la cuestión, se inclina por considerar que el licenciataria no es un verdadero «*Geheimnissinhaber*» (poseedor)⁸², sino un «*Geheimnisträger*», término con el que identifica a aquellas personas que han obtenido la información y tienen un control de hecho sobre la misma. Otra interpretación —opina— derivaría en una inflación inadmisibles de la legitimación activa, ya que la Directiva atribuye legitimación al poseedor del secreto⁸³.

Ohly, por su parte, afirma en un artículo de 2019, sin mayores explicaciones, que el poseedor del secreto empresarial puede ser quien haya generado la información, el cesionario o un licenciataria⁸⁴. En otro trabajo posterior, sin embargo, matiza su postura. Sostiene que atribuir legitimación activa al licenciataria podría poner en peligro el secreto (en el proceso judicial podría llegar a salir a la luz, a pesar de las cautelas adoptadas por la Ley), además de que una legitimación activa tan amplia, que no quedase siquiera limitada a determinados tipos de licencia, colisionaría con los principios del Derecho de la propiedad industrial e intelectual. Por estos motivos considera que el licenciataria no es «poseedor del secreto empresarial» en el sentido de la definición de la Directiva⁸⁵. A pesar de ello, no niega que pudiese trasladarse la solución que existe en determinados tipos de derechos de propiedad industrial e intelectual a este ámbito y conceder legitimación activa al licenciataria exclusivo, pero señala que la situación no es clara, y que en todo caso el poseedor del secreto podría prever en el contrato que las acciones solo se pudiesen ejercitar con su consentimiento⁸⁶.

En la misma obra, Harte-Bavendamm adopta una postura parecida a la de Ohly. Afirma que es necesario diferenciar entre los diversos tipos de licencia, y estima que cuando la licencia es exclusiva y el licenciante no puede explotar él mismo el secreto, el licenciataria sí ejerce un control legítimo sobre él (es poseedor, por tanto). En cualquier caso, recomienda que, en tanto el Tribunal de Justicia no se pronuncie, se establezcan en el contrato con precisión las facultades de las que dispone el licenciataria en caso de que se produzca una infracción

⁷⁸ *Ibid.*, pág. 709.

⁷⁹ Apdo. 13.

⁸⁰ En lugar de «*besitzt*» (posee [el control]), la Ley utiliza «*hat*» (tiene [el control]): «*jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat*» (§ 2.2).

⁸¹ Vid. HAUCK (2019), pág. 223 (puede ser poseedor, sin mayores precisiones); THIEL (2019), pág. 701 (puede ser poseedor, cuando ejerza el control); ALEXANDER (2022), *GeschGehG* § 2, apdo. 72 (es poseedor cuando pueda utilizar legítimamente el secreto); HIÉRAMENTE (2021), *GeschGehG* § 2, apdo. 82 (es poseedor cuando la licencia le permita utilizar y revelar el secreto).

⁸² Es el término que utiliza la versión alemana de la Directiva («*Inhaber eines Geschäftsgeheimnisses*»).

⁸³ MCGUIRE (2019), págs. 2217 y 2218. Siguen la opinión de esta autora HÖTTE (2021), § 10 *Haftung des Rechtsverletzers*, y HOHN-HEIN/BARTH (2021), *GeschGehG* § 2, apdo. 24.

⁸⁴ OHLY (2019), pág. 445.

⁸⁵ *Ibid.*, (2020), págs. 318 y 319.

⁸⁶ *Ibid.*, pág. 320.

que le concierna. De esta regulación contractual podría deducirse en qué medida el licenciataria ejerce el control legítimo sobre el secreto. Según el autor, el control legítimo del licenciataria no se puede afirmar o negar con carácter general, sino con la ayuda del tenor y finalidad del contrato de licencia en cuestión⁸⁷.

3. El debate en España

El asunto ha sido tratado en España a raíz de la decisión del legislador de utilizar el término «titular» en lugar del término «poseedor». El Anteproyecto ya optaba por esta terminología, y tanto el Dictamen del CGPJ, que dedicó unas amplias consideraciones a este cambio de nomenclatura⁸⁸, como el Dictamen del Consejo de Estado⁸⁹ se mostraron favorables al empleo del término «titular».

Dada la valoración positiva de los dos dictámenes no es de extrañar que la terminología del Anteproyecto se consolidase. La Exposición de Motivos señala al respecto que «[s]e ha considerado igualmente conveniente en todo caso preservar la terminología tradicionalmente empleada en nuestro sistema jurídico en los casos en los que los nuevos términos se refieren a conceptos sobradamente arraigados, estudiados y tratados en la legislación, la jurisprudencia y la doctrina. En este sentido, por ejemplo, se ha preferido mantener las expresiones de “secretos empresariales” para designar el objeto de protección y de «titular» para designar a quien legítimamente posee el secreto empresarial y se beneficia de su protección jurídica».

Como se puede observar, la Ley opta por el término titular, pero lo concibe de igual manera que la Directiva (el art. 1.2 dispone que: «La protección se dispensa al titular de un secreto empresarial, que es cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo»). Esta opción ha despertado diferentes valoraciones en la doctrina española.

Rabasa critica la equiparación, que le parece incorrecta, puesto que «en supuestos donde exista un licenciataria exclusivo que tenga reconocida contractualmente la facultad de conceder sublicencias, puede predicarse del mismo que ejerce un control sobre el derecho licenciado, pero en ningún caso la condición de titular, que corresponderá al licenciante»⁹⁰.

Guillén Monge trata de superar la discrepancia entre el término «poseedor» de la Directiva y el de titular de la Ley distinguiendo entre el «titular originario», que sería quien crea o desarrolla de manera independiente el secreto, y «titular derivativo», que es quien ejerce legítimamente el control del secreto bajo cualquier tipo de transmisión *inter vivos* o *mortis causa*. Entre los titulares derivativos encajarían «el empleador que es titular del secreto empresarial por cesión del trabajador, el licenciataria, el colaborador, el mandatario, etc.»⁹¹.

⁸⁷ HARTE-BAVENDAMM (2020), págs. 240 y 241. Parece haber cierta contradicción en las afirmaciones del autor. Creo no obstante que lo que afirma es que en el caso de una licencia simple el licenciataria no es poseedor, en el caso de licencia exclusiva en la que el licenciante no puede explotar él mismo el secreto sí, y en los demás casos habrá que interpretar el contrato de licencia para determinar, en virtud de su tenor y finalidad, si el licenciataria es poseedor.

⁸⁸ Puntos 59 y sigs.

⁸⁹ Pág. 42.

⁹⁰ RABASA (2018), epígrafe II. «Concepto de secreto».

⁹¹ GUILLÉN MONGE (2020, pág. 56). La autora hace referencia a la opinión de la Asociación de Expertos de Transferencia de Tecnología, LES España y Portugal, durante el trámite de consulta pública.

También la profesora Arroyo Aparicio se inclina por una interpretación amplia del término titular, pues considera que «puede ser el titular originario, único o cotitular, así como un licenciario que tenga derecho a realizar los actos que integran la utilización del secreto»⁹².

El profesor Gómez Segade, por su parte, ha señalado que el tenor del artículo 1.2 LSE «no parece demasiado preciso en la medida en que hay personas como los licenciarios exclusivos que ejercen legítimamente el control sobre el secreto, pero no son titulares del mismo»⁹³. Y en otro lugar afirma que «a pesar de lo que dice la LSE, no siempre el titular del secreto es quien ejerce el control sobre el mismo»⁹⁴. Es decir, que el profesor Gómez Segade considera que el término titular de la Ley y el poseedor de la Directiva no son equivalentes. Ello no quiere decir necesariamente, no obstante, que la Ley española contravenga la Directiva. El propio profesor considera, por ejemplo, que la alusión al titular que se hace en el artículo 1.1.c) es conforme con la Directiva⁹⁵.

El profesor Massaguer, por último, parece haber modificado su postura. En uno de sus trabajos parte de una posición maximalista, y considera que la condición de poseedor (en la Directiva) «concorre tanto en quien la adquirió originariamente, mediante su desarrollo, como en quien lo hizo en virtud de los derechos concedidos por el anterior, y entre estos últimos figura, sin duda, el licenciario, sea exclusivo o no exclusivo»⁹⁶. Sin embargo, en un artículo posterior sobre la LSE mantiene una interpretación divergente a la manifestada anteriormente. Considera ahora que «[e]l control sobre el secreto empresarial puede adquirirse, bien originariamente, mediante el descubrimiento o creación independiente de la información o conocimiento que constituyen su objeto [arg. ex art. 2.1.a) LSE], bien derivativamente, mediante la cesión (enajenación) del secreto empresarial (arg. ex arts. 4 I, 5.3 y 7 LSE), y ello tanto de forma individual como de forma conjunta entre varios (arg. ex art. 4.1 LSE). No sucede así, en cambio, mediante la sola concesión de una licencia, pues esta no determina la adquisición de la clase de control que sirve de asiento a la titularidad, sino solo una autorización limitada de utilización»⁹⁷. El profesor Massaguer parece que niega la condición de «poseedor» al licenciario, si bien es posible que se esté refiriendo únicamente al no exclusivo.

4. Opinión del autor

La Directiva no ha utilizado el término al que estamos habituados cuando nos movemos en el ámbito de la propiedad industrial, y que es por el que se decanta la Ley de Secretos Empresariales («titular»), sino que ha optado por el de «poseedor» del secreto empresarial. La propia Directiva define «poseedor de un

⁹² ARROYO APARICIO (2019), apdo. 25.

⁹³ GÓMEZ SEGADE (2019-2020), pág. 155.

⁹⁴ *Ibid.* (2020), pág. 144.

⁹⁵ *Ibid.* (2019-2020), pág. 154. Considera correcto que la LSE mencione únicamente al titular porque la Ley, al regular las licencias, impone al licenciario o sublicenciario la obligación de imponer las medidas necesarias para evitar la violación del secreto empresarial (art. 6.4). El profesor afirma que: «La Directiva, como no regula las licencias, para no excluir a los licenciarios tienen que utilizar el término omnicompreensivo como “la persona que legítimamente ejerza su control”».

⁹⁶ MASSAGUER (2018), epígrafe IV.2 («Infracción de secretos empresariales licenciados cometida por terceros»).

⁹⁷ MASSAGUER (2019), págs. 64 y 65.

secreto comercial» como «cualquier persona física o jurídica que legítimamente ejerza el control de un secreto comercial».

No entraña dificultad la referencia al ejercicio *legítimo* del control. El hecho de que el control deba ser «legítimo» permite descartar a los «detentadores», en el sentido ordinario de «Poseer o retener [algo, especialmente un título o cargo] ilegítimamente»⁹⁸, y no en el jurídico de «Tener, poseer, ser titular de algún bien o derecho»⁹⁹. El aspecto más interesante de la Directiva en este punto es que no habla de «poseedor legítimo», sino de «control legítimo». Es decir, que la legitimidad es un elemento de la definición, por lo que no existe «posesión» en ausencia de dicha legitimidad. Afirmar de una persona que es poseedor del secreto significa afirmar que es legítimo poseedor del mismo.

Mayores dificultades entraña determinar el otro elemento fundamental de la definición: el *ejercicio del control* sobre el secreto.

La Propuesta de Directiva¹⁰⁰ contiene una breve explicación sobre la opción adoptada: «La definición de «poseedor de un secreto comercial» retoma como elemento clave el concepto de legitimidad del control sobre el secreto comercial que figura igualmente en el Acuerdo sobre los ADPIC¹⁰¹. Se asegura así que el secreto comercial puede ser defendido no solo por el poseedor original, sino también por los licenciarios»¹⁰². La intención al optar por el término poseedor, por tanto, era ampliar el círculo de legitimados para la defensa del secreto. En efecto, en la medida en que la Directiva establece que «los Estados miembros garantizarán que *los poseedores de secretos comerciales* tengan derecho a solicitar las medidas, procedimientos y recursos previstos en la presente Directiva»¹⁰³, cuanto más dilatado sea el concepto de poseedor más amplio será el círculo de legitimados activamente.

La opción por la que se decantó la Propuesta (hablar de «poseedor», para así ampliar la legitimación) tampoco resulta extraña, si se tiene en cuenta que es la adoptada por el Derecho norteamericano, tan relevante en esta materia. En la aplicación de la *UTSA*, los tribunales consideran que no solamente está legitimado el propietario («*owner*»), sino también el poseedor¹⁰⁴, y la *Defend Trade Secrets Act* (DTSA) utiliza el término «*owner*», pero lo define de manera tan amplia que incluye al licenciario¹⁰⁵.

También una interpretación puramente gramatical aboga por una concepción que va más allá del titular. Por un lado, porque la Directiva no utiliza di-

⁹⁸ «Detentar» en el Diccionario panhispánico de dudas (<https://www.rae.es/dpd/detentar>).

⁹⁹ «Detentar» en el Diccionario Panhispánico del Español Jurídico (<https://dpej.rae.es/lema/detentar>).

¹⁰⁰ Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección del saber hacer y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y divulgación ilícitas. Bruselas, 28 de noviembre de 2013, COM(2013) 813 final. 2013/0402 (COD).

¹⁰¹ Artículo 39.2 Acuerdo ADPIC: «2. 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...».

¹⁰² Punto 5, «Explicación de la propuesta».

¹⁰³ Artículo 4.1: «Los Estados miembros garantizarán que los poseedores de secretos comerciales tengan derecho a solicitar las medidas, procedimientos y recursos previstos en la presente Directiva con el fin de impedir la obtención, utilización o revelación ilícitas de su secreto comercial o con el fin de obtener resarcimiento por ello».

¹⁰⁴ ALTMAN y POLLACK (2021), § 14:26, y JAGER (2021), § 5:6.

¹⁰⁵ «[T]he term “owner”, with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed», 18 U.S.C. § 1839 (4).

cho término, ni el de propietario («owner»), sino que se decanta por el término poseedor («holder»). Y, además, porque el concepto que ofrece de «poseedor» bascula sobre el término «control», que es el que habitualmente utilizan los países del *common law* para definir la posesión¹⁰⁶. Por otro lado, la Directiva habla de «cualquier persona»¹⁰⁷ («any natural or legal person», «jede natürliche oder juristische Person», «toute personne», «qualsiasi persona»), no de «la persona o personas», que hubiese sido más natural de haberse querido hacer referencia únicamente al titular¹⁰⁸. De hecho, la versión portuguesa, que diverge de las demás versiones (de lenguas que comprendo), sí usa el término titular, y no habla de «cualquier persona», sino de «a pessoa singular ou coletiva»¹⁰⁹.

Los argumentos ofrecidos hasta el momento permiten concluir que resulta incorrecto verter al español el término «poseedor» (*holder*, *Inhaber*, *detentore*, *détenteur*) como «titular», a no ser que se adopten las medidas legislativas adecuadas para asegurarse que quienes queden fuera del término titular, pero comprendidos en el de poseedor, tengan los derechos que les confiere la Directiva (como dispone el art. 288 TFUE, esta obliga en cuanto al resultado, dejando a las autoridades nacionales la elección de la forma y de los medios).

Dicho esto, algo hemos progresado, pero no demasiado, ya que aunque sabemos que el concepto de poseedor es más amplio que el de titular, seguimos necesitando delimitar su perímetro externo. Para ello puede ser útil realizar una interpretación de carácter sistemático. Si acudimos a la Directiva, observamos que el término poseedor se utiliza, con verdaderos efectos jurídicos, en dos momentos.

El primero es para otorgar legitimación a quien revista esta condición (art. 4.1) y el segundo es para configurar la ausencia de su voluntad como elemento constitutivo del ilícito (art. 4.2 y 3: la obtención, utilización y revelación que son ilícitas son las realizadas «sin el consentimiento de su poseedor»).

Ambos extremos son importantes, aunque no debemos caer en el error de realizar un razonamiento circular: no podemos decir que el poseedor es quien goza de legitimación o aquel cuya falta de consentimiento determina el ilícito, pues no habremos avanzado nada. Sin embargo, la interpretación sistemática sí que es relevante a ciertos efectos: pone de manifiesto el papel preeminente que la Directiva reserva al poseedor, como encargado de la tutela del secreto y como persona clave para determinar la licitud o ilicitud de la conducta. Y es esta reflexión la que permite descartar aquellas concepciones de poseedor que sean demasiado amplias, por una mera *reductio ad absurdum*. Resultaría absurdo, por ejemplo, considerar poseedor a toda persona en la que recaiga la mera tenencia de la información, sin ulteriores requisitos, pues el legislador no puede haber querido conferir legitimación y el poder de determinar la licitud o ilicitud

¹⁰⁶ «[P]ossession (14c) 2. The right under which one may exercise control over something to the exclusion of all others; the continuing exercise of a claim to the exclusive use of a material object» (definición del *Black's Law Dictionary*, 11.^a ed., 2019). «Possession. Actual control of property combined with the intention to use it, rightly or wrongly, as one's own. (...)». Definición de *A Dictionary of Law*, 9.^a ed., 2018, editado por Jonathan Law Publisher y Oxford University Press.

¹⁰⁷ GÖRG (2020), pág. 1515, apdo. 89, que apunta que la versión alemana utiliza el término «jede», y no «jene», aunque él lo pone en relación con la ausencia de derecho de exclusividad sobre los conocimientos técnicos o la información (cdo. 16 de la Directiva), en el sentido de que caben la «Doppelschöpfung» y la ingeniería inversa.

¹⁰⁸ En la versión portuguesa, sin embargo, se dice «a pessoa singular ou coletiva».

¹⁰⁹ Artículo 2.2: «“Titular do segredo comercial”, a pessoa singular ou coletiva que exerce legalmente o controlo de um segredo comerciais».

de la conducta a un mero tenedor del secreto, sin ulteriores consideraciones. Es decir, que el «control» al que se refiere la Directiva no se deriva de la mera «tenencia» de la información; es necesario un plus, una posición preeminente en relación con el secreto.

Esta posición preeminente la tendrá por supuesto el titular originario del secreto, o el cesionario del mismo. No la tendrán, por el contrario, aquellas personas a las que este titular confiera acceso al secreto bajo condiciones de confidencialidad, con obligación de reserva, como por ejemplo los trabajadores o colaboradores, y tampoco un licenciataria no exclusivo que no pueda conceder sublicencias y cuyas facultades se limiten a la utilización del secreto bajo las constricciones impuestas por el contrato de licencia. Todas estas personas se encuentran en una situación de plena subordinación frente al titular del secreto, que es quien delimita la esfera de actuación y las facultades de dichas personas, que quedan constreñidas por el contrato, y que no ejercen ningún control sobre el secreto, sino que actúan bajo el control de su titular.

La situación cambia, sin embargo, a medida que el contrato de licencia otorga mayores facultades al licenciataria, y se las arrebata al titular, de tal forma que en determinados contratos de licencia el control del secreto puede ser compartido por ambos contratantes, o incluso puede suceder que, cuando la posición del titular se vacía y sus facultades quedan muy limitadas, el control se desplace temporalmente (durante la vigencia del contrato) al licenciataria¹¹⁰. Resulta necesario, en definitiva, analizar el contrato de licencia para, caso por caso, y a la luz de las facultades conferidas a las partes, determinar si el control recae sobre el licenciante, sobre el licenciataria, o sobre ambos. Deberá hacerse una valoración global, aunque algunos extremos que pueden ser reveladores son los siguientes: si el licenciante conserva la facultad de utilizar el secreto, si puede conceder ulteriores licencias, si el licenciataria puede otorgar sublicencias, si para los actos anteriores se necesita la autorización de la otra parte, quién resulta legitimado, según el contrato, para el ejercicio de las acciones de defensa del secreto, quién puede otorgar, según el contrato, el consentimiento al que se refiere el artículo 4, apdos. 2 y 3 de la Directiva, etcétera.

Precisado así el concepto de poseedor, estamos ya en condiciones de determinar quién es la persona encargada de adoptar las medidas razonables, para lo cual conviene distinguir entre las medidas originarias y las posteriores.

Las medidas originarias no pueden adoptarse nunca por un licenciataria, ya que, en ausencia todavía de secreto, este no se ha podido licenciar. Las medidas, en este momento, deben ser adoptadas por el titular. Ahora bien, hablamos de medidas «originarias», puesto que el deber de mantener la información secreta se prolonga en el tiempo, por lo que si otras personas pasan a ser consideradas poseedores (por cesión, o por una licencia en la que la posición del licenciataria sea particularmente fuerte), entonces la carga recaerá (también, si hay otros poseedores, o únicamente, si no los hay) sobre ellas.

El licenciataria, por tanto, solo está obligado a la adopción de las medidas —como condición para que la información sea considerada secreto

¹¹⁰ COSTAS COMESAÑA (2020-2021, pág. 84, nota 19) indica, por ejemplo, que por medio de un contrato de licencia con cláusula de exclusiva y de duración indefinida o muy larga duración se puede conseguir *de facto* la misma función económica que con la cesión del secreto empresarial.

empresarial —¹¹¹ cuando, dada su posición contractual particularmente fuerte, pueda ser considerado poseedor del secreto. En otros casos, en los que el licenciario no sea poseedor, la Directiva no le obliga a adoptar las medidas necesarias para mantener la información secreta. Ahora bien, si no las adopta, la tutela del poseedor podría decaer, pero no como consecuencia directa de la no adopción de medidas por el licenciario, sino de manera indirecta, puesto que esa ausencia de medidas podría revelar, a su vez, la falta de adopción de medidas razonables por el verdadero poseedor. El licenciante debe controlar, por vía contractual y de *enforcement*, que el licenciario adopte medidas para mantener la información secreta. No hacerlo puede provocar que la protección decaiga, debido a su negligencia o pasividad (incumple el «deber de diligencia en lo que respecta al mantenimiento de la confidencialidad de su valioso secreto comercial» al que se refiere el considerando 23 de la Directiva).

Otros escenarios también son factibles: puede que el licenciario sea el poseedor, y el licenciante, cuya posición jurídica se haya visto prácticamente vaciada, no. En estos casos las medidas razonables deben ser adoptadas por el licenciario (pero, al igual que en el caso anterior, si el licenciante no las adopta podría decaer la protección por la pasividad del licenciario, desde su atalaya de control, al no exigir que el licenciante sea diligente en la custodia de la información). Y puede suceder, por último, que tanto el licenciante como el licenciario sean poseedores, y entonces la obligación recae directamente sobre ambos, y el demandado puede alegar que cualquiera de ellos ha incumplido su deber para lograr que la protección decaiga, sin necesidad de argumentar que el hecho de que el licenciario no haya adoptado las medidas constituye un incumplimiento del deber de la adopción de medidas por parte del licenciante.

XI. BIBLIOGRAFÍA

- ALEXANDER, Christian (2017), «Der Schutz von Geschäftsgeheimnissen nach der RL (EU) 2016/943», *WRP* 9, págs. 1034-1045.
- (2022), «Gesetz zum Schutz von Geschäftsgeheimnissen», en KÖHLER, Helmut; BORNKAMM, Joachim; FEDDERSEN, Jörn, y ALEXANDER, Christian, *UWG*, 40.^a ed., base de datos *beckonline*.
- ALTMAN, Louis, y POLLACK, Malla (2021), «§ 14:26. Required relationship to plaintiff», en *Callmann on Unfair Comp., Tr. & Mono.* (4.^a ed.), actualización de diciembre de 2021, base de datos *Westlaw Classic*.
- ARROYO APARICIO, Alicia (2019), «Secretos Empresariales en el ordenamiento español», *Revista Aranzadi Doctrinal* 11, BIB 2019\9602, base de datos *Aranzadi Westlaw*.
- BONE, Robert G. (1998), «A New Look at Trade Secret Law: Doctrine in Search of Justification», *Cal. L. Rev.*, vol. 86, núm. 2, págs. 241-314.

¹¹¹ La LSE dispone que: «El licenciario o sublicenciario estará obligado a adoptar las medidas necesarias para evitar la violación del secreto empresarial» (art. 6.4). Pero no se trata, en mi opinión, de una exigencia para la existencia de un secreto empresarial. Si el licenciario no es poseedor en el sentido de la Directiva, no puede imponerse esta exigencia porque contravendría el Derecho de la Unión. La Directiva no concede margen de actuación en lo que al concepto de secreto empresarial se refiere (edo. 14: «Es importante formular una definición homogénea del término “secreto comercial”») y mucho menos para restringir la protección. Cosa distinta es el que si el licenciario o sublicenciario no poseedor no adopta «las medidas necesarias para evitar la violación del secreto empresarial» pueda incurrir en responsabilidad frente al titular.

- (2011), «Trade secrecy, innovation and the requirement of reasonable secrecy precautions», en DREYFUSS, R. C., y STRANDBURG, K. J. (eds.), *The law and theory of trade secrecy: a handbook of contemporary research*, Edward Elgard, Cheltenham y Northampton, págs. 46-76.
- CALLMANN, Rudolf (1968), *Unfair Competition Trademarks and Monopolies*, 3.^a ed., Mundelein.
- COSTAS COMESAÑA, Julio (2020-2021), «La transmisibilidad del secreto empresarial», *ADI* 41, págs. 79-108.
- CUNDIFF, Victoria A. (2009), «Reasonable Measures to Protect Trade Secrets in a Digital Environment», *IDEA* 49, págs. 359-410.
- DOLE, Richard F. Jr. (2016), «The Contours of American Trade Secret Law: What Is and What Isn't Protectable as a Trade Secret», *SMU Science and Technology Law Review*, vol. 19, núm. 2, págs. 89-124.
- FERNÁNDEZ CARBALLO-CALERO, Pablo (2013), «La configuración del listado de clientes como un secreto empresarial en el Derecho contra la competencia desleal», en TOBÍO RIVAS, A. M.^a; FERNÁNDEZ-ALBOR BALTAR, A., y TATO PLAZA, A. (eds.), *Estudios de Derecho Mercantil. Libro homenaje al prof. Dr. Dr. h. c. José Antonio Gómez Segade*, Marcial Pons, Madrid, págs. 411-419.
- (2020), «La aportación del “know-how” al capital social (Comentario a la Resolución de la Dirección General de los Registros y del Notariado de 4 de diciembre de 2019)», *RdS* 59, base de datos *Aranzadi Westlaw*.
- GÓMEZ SEGADE, José Antonio (1974), *El secreto industrial (Know-how). Concepto y protección*, Tecnos, Madrid.
- (2019-2020), «La nueva ley de secretos empresariales», *ADI* 40, págs. 141-164.
- (2020), «La protección de los macrodatos (big data) mediante las normas sobre secretos empresariales», en GARCÍA VIDAL, Á. (dir.), *Big data e internet de las cosas: nuevos retos para el derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch, Valencia, págs. 115-152.
- GÖRG, Mathias (2020), *Kommentar zum UWG*, LexisNexis, Wien.
- GULLÉN MONGE, Patricia (2020), «Capítulo I. Disposiciones generales», en LISSÉN ARBELOA, J. M. (coord.), *Comentario a la Ley de Secretos Empresariales*, La Ley Wolters Kluwer, Madrid, págs. 33-61.
- HARTE-BAVENDAMM, Henning (2020), «§ 2 Begriffsbestimmungen», en HARTE-BAVENDAMM, Henning; OHLY, Ansgar, y KALBFUS, Björn), *GeschGehG*, C.H. Beck, München, págs. 197-253.
- HAUCK, Ronny (2019), «Was lange währt... - Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist in Kraft», *GRUR-Prax* 10, págs. 223-225.
- HIÉRAMENTE, Mayeul (2021), «GeschGehG § 2 Begriffsbestimmungen», en FUHLROTT, Michael, e HIÉRAMENTE, Mayeul, *BeckOK GeschGehG*, 10.^a ed., base de datos *beckonline*.
- HOEREN, Thomas (2021), «§ 2 Begriffsbestimmungen», en HOEREN, Thomas, y MÜNKER, Reiner, *GeschGehG - Gesetz zum Schutz von Geschäftsgeheimnissen*, De Gruyter, Berlin, Boston, págs. 61-77.
- HOHN-HEIN, Nicolas, y BARTH, Günter (2021), «GeschGehG § 2 Begriffsbestimmungen», en FRITZSCHE, Jörg; MÜNKER, Reiner, y STOLLWERCK, Christoph, *BeckOK UWG*, 14.^a ed., base de datos *beckonline*.
- HÖTTE, Daniel Antonius (2021), «§ 10 Haftung des Rechtsverletzers», en HOEREN, Thomas, y MÜNKER, Reiner, *GeschGehG - Gesetz zum Schutz von Geschäftsgeheimnissen*, De Gruyter, Berlin-Boston, 2021, págs. 303-317.
- JAGER, Melvin F. (2021), *Trade Secrets Law*, actualización de octubre de 2021, base de datos *Westlaw Classic*.
- KALBFUS, Björn (2016), «Die EU-Geschäftsgeheimnis-Richtlinie», *GRUR* 10, págs. 1009-1017.
- (2017A), «Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie», *GRUR-Prax* 10, págs. 391-393.

- (2017B), «UWG § 17 Verrat von Geschäfts- und Betriebsgeheimnissen», en FRITZSCHE, Jörg; MÜNKER, Reiner, y STOLLWERCK, Christoph, *BeckOK UWG*, 4.^a ed., base de datos *beckonline*.
- KÖHLER, Helmut (2018), «§ 17 Verrat von Geschäfts- und Betriebsgeheimnissen», en KÖHLER, Helmut; BORNKAMM, Joachim, y FEDDERSEN, Jörn, *UWG*, 36.^a ed., base de datos *beckonline*.
- LEISTER, Alexander (2019), «Angemessene Geheimhaltungsmaßnahmen - Handlungsbedarf in der Praxis durch Neudefinition des Geschäftsgeheimnisbegriffs», *GRUR-Prax* 4, págs. 75-77.
- MAAßEN, Stefan (2019), «“Angemessene Geheimhaltungsmaßnahmen” für Geschäftsgeheimnisse», *GRUR* 4, págs. 352-360.
- MASSAGUER, José (2018), «El incumplimiento de los contratos de licencia de patente y de licencia de secretos empresariales: concurrencia entre acciones contractuales y acciones por infracción», *RDM* 309, 2018, BIB 2018\12345, epígrafe «2. Infracción de secretos empresariales licenciados cometida por terceros», BIB 2018\12345, base de datos *Aranzadi Westlaw*.
- (2019), «De nuevo sobre la protección jurídica de los secretos empresariales (A propósito de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales)», *Actualidad Jurídica Uría Menéndez* 51, págs. 46-70.
- MCGUIRE, Mary-Rose (2019), «§ 2 GeschGehG», en BÜSCHER, W., *Gesetz gegen den unlauteren Wettbewerb Kommentar*, Heymanns, Köln, págs. 2204-2220.
- MILGRIM (2002-; hojas sueltas), *Milgrim on Trade Secrets*, Lexis Nexis, New York.
- NEALEY, Tara; DAIGNAULT, Ronald M., y CAI, Yu (2015), «Trade Secrets in Life Science and Pharmaceutical Companies», *Cold Spring Harbor Perspectives in Medicine*, 5:a020982, disponible en <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4382727>.
- OHLY, Ansgar (2014), «Der Geheimnisschutz im deutschen Recht: heutiger Stand und Perspektiven», *GRUR* 1, págs. 1-11.
- (2019), «Das neue Geschäftsgeheimnisgesetz im Überblick», *GRUR* 5, págs. 441-451.
- (2020), «§ 6 Beseitigung und Unterlassung», en HARTE-BAVENDAMM, Henning; OHLY, Ansgar, y KALBFUS, Björn, *GeschGehG*, C. H. Beck, München.
- RABASA MARTÍNEZ, Ignacio (2018), «El anteproyecto de Ley de Secretos Empresariales y la Directiva 2016/943 relativa a los conocimientos técnicos e información empresarial no divulgados», *La Ley mercantil* 47 (mayo), págs. 5 y sigs.
- SANDEEN, Sharon K. (2010), «The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act», *Hamline Law Review*, vol. 33, núm. 3, págs. 493-544.
- (2014), «Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection», *Virginia Journal of Law & Technology*, vol. 19, núm. 1, págs. 1-103.
- SLABY, David W.; CHAPMAN, James C., y O'HARA, Gregory P. (1989), «Trade Secret Protection: An Analysis of the Concept Efforts Reasonable Under the Circumstances to Maintain Secrecy», *Santa Clara J.C.H.T.*, vol. 5, núm. 2, págs. 321-348.
- SUÑOL LUCEA, Aurea (2009), *El secreto empresarial. un estudio del artículo 13 de la Ley de Competencia Desleal*, Thomson Reuters Civitas, Cizur Menor.
- (2020-2021), «La protección de los datos como secreto empresarial en la era de la inteligencia artificial», *ADI* 41, págs. 193-218.
- THIEL, Linda (2019), «Das neue Geschäftsgeheimnisgesetz (GeschGehG) - Risiken und Chancen für Geschäftsgeheimnisinhaber», *WRP* 6, págs. 700-703.
- TRALLERO OCAÑA, Teresa (2021), *The Notion of Secrecy*, Nomos, Baden-Baden.
- TREBECK, Joachim, y SCHULTE-WISSERMANN, Lisa (2018), «Die Geheimnisschutzrichtlinie und deren Anwendbarkeit», *Neue Zeitschrift für Arbeitsrecht* 18, págs. 1175-1180.

- VANDEVELDE, Kenneth J. (1980), «The New Property of the Nineteenth Century: The Development of the Modern Concept of Property», *Buffalo Law Review*, vol. 29, núm. 2, págs. 325-367.
- VARADARAJAN, Deepa (2017), «Trade Secret Precautions, Possession, and Notice», *Hastings Law Journal*, vol. 68, núm. 2, págs. 357-396.
- WÜRTEMBERGER, Gert, y FREISCHEM, Stephan (2018), «Stellungnahme zum Referententwurf des Bundesministeriums der Justiz und für Verbraucherschutz - Entwurf eines Gesetzes zur Umsetzung der RL 2016/943/EU zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung», *GRUR* 7, págs. 708-713.