Francisco Martínez Rivas

LA CONFIGURACIÓN DEL DELITO DE REVELACIÓN DE SECRETOS EN EL ÁMBITO EMPRESARIAL

Atelier
LIBROS JURÍDICOS

La configuración del delito de revelación de secretos en el ámbito empresarial

La configuración del delito de revelación de secretos en el ámbito empresarial

Francisco Martínez Rivas

Atelier
LIBROS JURÍDICOS

Este libro ha sido sometido a un riguroso proceso de revisión por pares.

Santa Dorotea 8, 08004 Barcelona
e-mail: atelier@atelierlibros.es
www.atelierlibrosjuridicos.com
Tel. 93 295 45 60

I.S.B.N.: 979-13-87867-94-2
Depósito legal: B 21906-2025

Diseño y composición: Addenda, Pau Claris 92, 08010 Barcelona
www.addenda.es

Impresión: Podiprint

SUMARIO

1. INTRODUCCIÓN

La aparición de nuevos mecanismos susceptibles de ser utilizados para la captación de secretos e informaciones personales y empresariales, debido al incremento del desarrollo tecnológico, hace necesario realizar un estudio concreto y detallado de los sistemas que el ordenamiento ofrece para que la información empresarial quede debidamente protegida frente a las posibilidades de captación por terceros no autorizados para ello.

La tecnología ofrece, a medida que se va desarrollando e implantando en nuestra sociedad de manera generalizada, nuevos métodos aptos para ser utilizados en el descubrimiento de informaciones y secretos empresariales. Aunque las conductas de captación y revelación pueden referirse a datos personales relativos a la intimidad y a la esfera privada de los individuos, también es posible que estas conductas se realicen con la intención de obtener la información que opera en manos de una empresa. Los conocimientos específicos adquiridos por ésta en el desarrollo de sus competencias profesionales son a veces un reclamo demasiado tentador para aquellos que buscan adquirir ese conocimiento sin haber empleado el esfuerzo económico, formativo y laboral que la empresa necesitó para llegar a tal conocimiento.

El ordenamiento jurídico debe proteger que la competencia empresarial se realice respetando el desarrollo de las actividades empresariales dentro de los términos previstos por la ley, imposibilitándose conductas que resulten atentatorias contra la

libertad de empresa y la protección de sus derechos económicos. El derecho de toda empresa a desarrollar su actividad, adquiriendo conocimientos que le permitan ostentar una posición más prevalente en el mercado, debe ser protegido por el legislador. No puede desconocerse el derecho a que las informaciones y conocimientos técnicos adquiridos en el ámbito de una empresa deban ser salvaguardados. Ni obviarse que el desarrollo de tales conocimientos es susceptible de ser explotados económicamente por la empresa, y siempre habrá un interés por parte de terceros competidores en obtener tal información para ser usada en su propio beneficio.

La tipificación en el Código Penal de las conductas que impliquen descubrir o apoderarse de secretos de empresa ha sido una de las vías más loables para evitar los perjuicios económicos que la empresa puede sufrir como consecuencia de que los secretos que operan sólo en el ámbito empresarial sean conocidos por terceros. Siendo este tercero una empresa perteneciente a la competencia, resulta claro que, con tal conducta de captación y revelación de secretos, se entorpece el avance en el mercado de la empresa cuyo secreto ha sido sustraído, pero también se la perjudica económicamente dado que limita los resultados de su actividad en beneficio de la competencia.

Como veremos, el delito de revelación del secreto castiga el acceso, revelación, difusión o utilización de una información empresarial, tipificando la conducta de aquellos que buscan el descubrimiento y revelación de tal información para obtener beneficios derivados de su uso, sin haber realizado un esfuerzo propio en aras a alcanzar el conocimiento científico o empresarial en el que el secreto revelado consiste.

Es absolutamente indispensable que las empresas vean garantizado el derecho a progresar dentro del mercado de acuerdo con sus capacidades y su esfuerzo. El legislador debe ofrecer todos los mecanismos a su alcance para que no se incurra en conductas de competencia desleal, que infringen los principios de funcionamiento del mercado y afecten a la capacidad competitiva de las empresas. Obtener indebidamente secretos de empresa, difundirlos o divulgarlos a terceros, o utilizarlos

de forma que se obtengan ventajas directas o indirectas, debe ser castigado penalmente. Si las conductas de descubrimiento de secretos y vulneración de intimidad es castigada por el legislador penal en el artículo 197 del Código Penal, dentro de los denominados «delitos de descubrimiento y revelación de secretos», también es necesario que el legislador proteja el derecho de las empresas a utilizar los conocimientos técnicos que favorezcan su desarrollo en el mercado en función de sus propios méritos, eficiencia y productividad, sin sufrir ningún tipo de injerencia o intento de sustracción. El bagaje científico y empresarial que una empresa adquiere, como consecuencia del desarrollo de sus actividades, debe entenderse que forma parte de su propio patrimonio y capital. De ahí que se requiera no sólo una protección a nivel civil, que indemnice a la empresa por los daños causados, sino una protección penal que tipifique las conductas que atenten contra el patrimonio inmaterial de la empresa, sus conocimientos y desarrollo empresarial. Además, con las conductas de revelación de secretos de empresa no sólo se afecta económicamente a la empresa cuyo secreto ha sido revelado. La propia sociedad en su conjunto puede verse perjudicada cuando el descubrimiento de ciertos datos y secretos que habilitaban a una empresa a ocupar una posición preponderante en el mercado altera de manera efectiva el sistema de oferta y demanda.

Lógicamente en nuestra sociedad no puede ponerse obstáculos al desarrollo tecnológico, pues ha sido éste el que nos ha permitido alcanzar cuotas de bienestar nunca antes imaginadas. Sin embargo, es cierto que con el desarrollo de la tecnología se han ofrecido mecanismos novedosos, que con el mínimo esfuerzo, permiten acceder a un nivel de información y datos inimaginable. Poner coto a las conductas que aprovechen la tecnología para la obtención de secretos determinantes de la competitividad de una empresa, es labor del legislador. A mayores ha de tenerse en cuenta que la configuración actual de la sociedad, que nos obliga a manejar cantidades ingentes de datos de manera eficiente, nos hace imprescindible acudir al uso de medios tecnológicos para poder tratar los datos eficazmente

y con la rapidez que la sociedad requiere. Ello conlleva que la totalidad de empresas, privadas y públicas, se vean obligadas a poner su información en soportes telemáticos, dada la imposibilidad de gestionar los mismos en soporte físico, lo que deja claramente patente la vulnerabilidad de la empresa a nivel de seguridad. Toda la información relevante para ella es susceptible de ser conocida y utilizada si se usan métodos ilícitos que permiten su acceso y difusión. Aunque el empresario tiene obligación de adoptar todas las medidas de seguridad necesarias para que esto no suceda, el legislador ha de colaborar en su protección tipificando penalmente estas conductas atentatorias contra la libertad de empresa y competencia.

A lo largo de estas páginas, realizaremos un estudio detallado del delito de revelación de secretos de empresa. Aunque nos centraremos en las especificidades propias de la realización de esta conducta en el ámbito de la empresa privada, lo cierto es que la tipificación de estos delitos en los artículos 278 y siguientes del Código Penal, nos remite en su articulado a los «delitos de revelación y descubrimiento de secretos» previstos en los artículos 197 y siguientes del mismo texto. Por ello, en muchas ocasiones, para poder hacer una adecuada definición de las conductas tipificadas, se hará necesario acudir a la regulación de los delitos de descubrimiento y revelación de secretos y datos relativos a la intimidad de las personas. Es cierto que ambos delitos, los de revelación de secretos personales y los de revelación de secretos empresariales, tienen como punto en común la protección de aspectos integrados en el ámbito más privado del individuo o el más interno de la empresa. La posibilidad de acceder, sin el consentimiento del titular de los datos, a informaciones y conocimientos que entran dentro de la esfera privada debe ser castigado por el legislador penal. Esos datos, que en unas ocasiones afectan a la intimidad personal y familiar del individuo, y en otras a informaciones y conocimientos adquiridos exclusivamente en el ámbito empresarial, han de ser debidamente protegidos por el ordenamiento y poner coto a las conductas de acceso, uso o divulgación de los mismos es absolutamente indispensable. Y sobre todo desde que la tecnología ha

facilitado la obtención y el uso indebido de esos datos mediante la utilización de métodos cada vez más accesibles y sencillos.

No son baladís las consecuencias económicas y limitativas de la competencia empresarial derivadas de las conductas ilícitas consistentes en la obtención, revelación o utilización de informaciones o secretos empresariales. De la misma forma que la obtención y uso de datos personales afecta a la intimidad y a la esfera privada de los individuos protegida constitucionalmente, también la empresa tiene derecho a la libertad de empresa y al desarrollo de su capacidad competitiva reconocida por el constituyente. Este derecho se hace efectivo cuando a la empresa se le garantiza un adecuado desarrollo de sus actividades empresariales dentro del mercado, y una adecuada protección para que los conocimientos adquiridos tras el esfuerzo económico de la empresa y el laboral de sus empleados, sean utilizados en su beneficio y desarrollo.

El esfuerzo financiero y laboral que supone adquirir ciertas informaciones y conocimientos favorece a su vez la innovación empresarial. La competitividad y mayor productividad de las empresas que deviene de la posesión de tales conocimientos debe ser debidamente salvaguardada, de forma que las empresas en el mercado actúen en función de esos conocimientos y de sus méritos y capacidades, tipificándose las conductas de aquellos que se benefician de secretos obtenidos ilícitamente.

El valor empresarial de los secretos alcanzados por una empresa es incuestionable, si tenemos en cuenta que de su posesión y uso deviene el desarrollo económico y el posicionamiento de una empresa en el mercado. La tipificación de las conductas de descubrimiento y revelación garantiza que la investigación y el progreso técnico se realicen de manera coherente con el esfuerzo requerido para alcanzar tales conocimientos.

El presente trabajo será un intento de delimitar los elementos constitutivos del tipo delictivo de revelación de secretos de empresa contemplado en el artículo 278 del Código Penal. Analizar los elementos subjetivos y objetivos que son necesarios para entender que la conducta constituye un hecho delictivo, es indispensable para poder definir cuando el acceso, revelación o

uso de datos empresariales puede ser considerado un delito. Y uno de los elementos que requieren ser concretados de forma específica es el concepto de secreto empresarial. Hemos de analizar qué tipo de información podemos entender incluida en este término, delimitando los contornos del concepto en función de las aportaciones doctrinales y jurisprudenciales. El hecho de que el «secreto empresarial» sea un elemento esencial para una adecuada definición del delito de revelación de secretos en el ámbito de la empresa, nos obliga a su adecuada conceptualización y delimitación. De si la información indebidamente obtenida o divulgada es susceptible de ser calificada como secreto de empresa o no, dependerá que se proceda a la aplicación de los artículos 278 a 280 del Código Penal, o en caso de no serlo, de los artículos 197 y siguientes.

Sin perjuicio de que lo estudiemos con mayor de entretenimiento, y en aras de sentar las bases de nuestro estudio, podemos entender por secreto empresarial toda aquella información secreta que directamente relacionada con la actividad de una empresa, le confiere y atribuye de manera clara una ventaja en la competencia, de manera que el conocimiento y uso de ese secreto exclusivo le facilita posicionarse preferentemente con respecto al resto de las empresas del mercado.

Aunque realizaremos una mayor concreción en las páginas siguientes, es necesario en estos primeros momentos, recordar que son principalmente tres las conductas tipificadas en los artículos 278 a 280 del Código Penal. En primer lugar, el espionaje industrial previsto en el artículo 278.1, que consiste en apoderarse ilegítimamente de un secreto empresarial y que es castigado con mayor gravedad en el caso de que una vez obtenido el conocimiento del secreto, se proceda a su difusión, revelación o cesión a terceros. Esta última conducta es tipificada como un supuesto agravado en el artículo 278.2 del Código Penal. La segunda conducta que entraría dentro de la considerada revelación de secretos empresariales son las previstas en el artículo 279. En este precepto se hace referencia a la vulneración del deber de guardar secreto ocasionada como consecuencia de la comunicación de la información a terceros ajenos a la misma (apartado 1) y al uso de

un secreto empresarial en provecho propio (apartado 2). La tercera de las modalidades se concreta en el artículo 280 y tipifica las conductas de «uso en provecho propio o revelación de la información con conocimiento de su origen ilícito».

Estas conductas tipificadas por el legislador protegen los secretos empresariales y posibilitan que las leyes del mercado sean garantía de que la competencia se desarrolle en base a criterios de lealtad. De esta forma, basando el desarrollo del mercado en la lealtad competencial, el mérito y la igualdad, serán sólo la minimización de los costes y la capacidad de la empresa a la hora de diferenciar su producto con respecto a la competencia, los elementos que determinen la capacidad de desarrollo empresarial en el mercado. Lógicamente los secretos de empresa afectan de manera directa a la capacidad de diferenciación del producto o servicio ofrecido. Diferenciar ese producto de las características generales ofrecidas por la mayoría de la competencia, puede ser determinantes a la hora de alcanzar una posición prioritaria en el mercado. Los secretos empresariales resultan indispensables para que la estrategia de diferenciación resulte efectiva. Si el conocimiento o secreto que posibilita a la empresa diferenciar a su producto del resto, alcanza un general conocimiento, se frustran plenamente las posibilidades de desarrollo de la empresa en el mercado y hará imposible que este alcance una posición puntera en el sector al que pertenece.

La ventaja competitiva que todo secreto empresarial conlleva es la razón de que la información se mantenga en secreto. El conocimiento general del mismo frustra las estrategias empresariales y el desarrollo económico de la empresa. Y si ese conocimiento ha sido alcanzado como consecuencia de un esfuerzo de investigación y desarrollo, mayores razones hay para mantener en secreto esa información. Supondría invertir en alcanzar un conocimiento, para que después, en el caso de que sea conocido por terceros, no redunde en beneficio directo de la empresa que ha invertido económicamente en alcanzar tal conocimiento.

Si analizamos el comportamiento del mercado en los últimos años, podemos observar que han sido varios los casos en los que la violación de secretos empresariales ha ocasionado

innumerables pérdidas económicas. La inversión en I+D puede verse completamente frustrada como consecuencia de la revelación de secretos empresariales y las cifras de pérdidas de billones de dólares en Estados Unidos, y miles de millones de euros en Europa justifica la necesidad de que el legislador delimite de manera clara qué deba entenderse por secreto profesional y cuáles deban ser los mecanismos para que los secretos de empresa sean debidamente protegidos.

Por otra parte, ha de recordarse que los delitos de revelación de secretos empresariales no sólo protegen los derechos de la empresa. El Estado también tiene interés en que el mercado se desarrolle con arreglo a criterios de igualdad y justicia, de manera que el avance económico de las empresas se fundamente en el esfuerzo y el trabajo, sin que resulten admisibles conductas que perturben los principios de funcionamiento de la libertad de empresa y del mercado. Si el Estado no ofrece suficiente protección a las empresas para que sus secretos queden protegidos, se obligaría a las mismas a adoptar costosas medidas para su autoprotección a fin de que la información y el conocimiento que estuvieran en posesión de la empresa no pudieran ser conocidos por terceros. La falta de protección y control sobre la información por parte de la empresa, de no ser tipificadas las conductas de revelación de secretos empresariales, le obligaría a invertir parte de su capital en mecanismos de defensa de sus secretos, y, en consecuencia, se limitaría el desarrollo tecnológico y la inversión en la innovación.

En consecuencia, la no intervención del Estado en la tipificación de las conductas ocasionaría una pérdida de competitividad y una limitación de las capacidades económicas de la empresa para la inversión en I+D. Como se recuerda en el documento del Ministerio de Economía y Competitividad titulado «Estrategia Española de Ciencia, Tecnología e innovación 2013-2020»[1], «la investigación científica y técnica, el desarrollo y la innovación

1. MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD. «Estrategia Española de Ciencia, Tecnología e innovación 2013-2020». Recurso electrónico disponible

constituyen factores indispensables para el crecimiento económico de un país y son la base de su progreso y bienestar sociales.»

A nivel europeo también se ha sido consciente de esta realidad. De hecho, en la «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», de 28 noviembre de 2013[2] se hace mención del asunto en su considerando 3 al establecer lo siguiente.

> «La ausencia de medios jurídicos efectivos y comparables para proteger los secretos comerciales en toda la Unión menoscaba los incentivos para emprender actividades transfronterizas innovadoras en el mercado interior e impiden que los secretos comerciales puedan liberar su potencial como motores del crecimiento económico y del empleo. Así pues, la innovación y la creación se ven desincentivadas y disminuye la inversión, con los consiguientes efectos en el buen funcionamiento del mercado interior y la consiguiente merma de su potencial como factor de crecimiento».

El Estado busca mejorar el bienestar de los ciudadanos y favorecer el incremento de su nivel de vida. Si las empresas no ven protegidos sus secretos profesionales se afectaría de manera directa la competitividad, y se limitarían los beneficios económicos de las empresas no sólo en el ámbito nacional sino también internacional. La reducción en los beneficios de la empresa limitaría sus posibilidades de inversión en la innovación

---

en: https://www.ciencia.gob.es/dam/jcr:49a4ab93-ce39-4034-bdaf-e3bf999cb51f/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf

2. Publications Office of the European Union. (2013, 28 noviembre). 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, /* COM/2013/0813 final - 2013/0402 (COD) */, CELEX1. Publications Office Of The EU. Recurso electrónico disponible en: https://op.europa.eu/en/publication-detail/-/publication/0e7bac3f-5c28-11e3-914b-01aa75ed71a1/language-es

y se frenaría ese objetivo de favorecer y mejorar las condiciones de vida de los ciudadanos.

Una vez introducida la necesidad de estudiar la materia con detenimiento, realizar una delimitación exacta de los contornos del delito de revelación de secretos empresariales es absolutamente indispensable. Habremos de determinar en qué momentos podemos considerar que el secreto de empresa ha sido infringido y cuándo, sin embargo, conductas como la utilización de los secretos de empresa por parte de uno de sus trabajadores, no son susceptibles de ser tipificados. Lógicamente los trabajadores, con acceso directo a los secretos empresariales, tienen entre sus obligaciones laborales, tal como se dispone en el artículo 5.e) del Estatuto de los Trabajadores aprobado por «Real Decreto Legislativo 2/2015, de 23 de octubre», contribuir a mejorar la productividad y favorecer el desarrollo de la empresa[3]. A veces ese desarrollo requiere que los conocimientos y secretos integrados en las bases de datos de la empresa, sean utilizados y conocidos por los trabajadores a los efectos de alcanzar los objetivos laborales implantados por la empresa. Estas conductas de acceso y uso de los datos por parte de los trabajadores en el ejercicio de sus relaciones laborales, no entra por supuesto dentro del tipo penal del delito de revelación de secretos. No obstante, en muchas ocasiones, la empresa intenta proteger las informaciones, datos y secretos que se hallan en su poder, sometiendo al trabajador a un acuerdo de confidencialidad. De esta manera se evita que el trabajador pueda poner fin a las relaciones laborales con la empresa y comenzar a prestar sus servicios a favor de empresarios de la competencia, con el consiguiente peligro de que pueda hacer uso de la información

3. Art. 5 e) Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. «BOE» núm. 255, de 24 de octubre de 2015, páginas 100224 a 100308 (85 págs.) «Los trabajadores tienen como deberes básicos: […] Contribuir a la mejora de la productividad».

y conocimientos previamente alcanzados, o proceda incluso a la revelación de los mismos a su nuevo contratante.

Como vemos, son muchas las razones para realizar un estudio detallado del delito de revelación de secretos. Intentaremos aportar luz sobre las problemáticas derivadas de su aplicación y delimitaremos las características y elementos que han de concurrir en las conductas delictivas para poder considerarlas incluidas dentro del tipo penal objeto de estudio en este trabajo. Acudir a las bases de datos legales y a la normativa aplicable en materia de competencia y revelación de secretos, en el ámbito civil y mercantil, así como en el penal, ha sido indispensable para alcanzar una visión de conjunto sobre los mecanismos de protección ofrecidos por el legislador español con respecto a los secretos empresariales.

Las aportaciones jurisprudenciales en la delimitación de las instituciones jurídicas son absolutamente indispensables para que el estudio de cualquier concepto jurídico sea completo. Las sentencias aportadas por el Tribunal Supremo nos han permitido alcanzar un conocimiento más exacto de las peculiaridades y particularidades del delito de revelación de secretos. El análisis de múltiples resoluciones judiciales nos ha permitido conocer las bases sobre las que se asienta la regulación del delito y los principios jurídicos que motivaron al legislador a tipificar las conductas. La jurisprudencia analizada ha sido útil para poder delimitar y diferenciar, siendo conscientes de que existen características comunes que los unen, los delitos de descubrimiento y revelación de secretos que afectan a la intimidad de los individuos previstos en el artículo 197 y siguientes del Código Penal, de los delitos de descubrimiento y revelación de secretos de empresa propiamente dichos, que serán los que serán objeto de estudio en este trabajo.

Como consecuencia de la utilización de todos estos instrumentos, normativos, doctrinales y jurisprudenciales, y en base al conocimiento adquirido, intentaremos ofrecer un análisis completo del delito de revelación de secretos de empresa. Pondremos de manifiesto los elementos objetivos y subjetivos del tipo delictivo, las circunstancias relativas a la culpabilidad y las

cuestiones penológicas. Se realizará un análisis del concepto de secreto empresarial, y de la aportación de jurisprudencia y doctrina en la definición de este término. A su vez se delimitarán de forma clara las modalidades de esta conducta delictiva, haciendo hincapié en aquellas circunstancias que legitimen una agravación en la imposición de la pena como consecuencia de una mayor afectación del bien jurídico protegido.

Por último, cabe mencionar que los delitos contra el mercado y los consumidores pueden definirse como infracciones de carácter socioeconómico cuya tipificación legal tiene por objeto sancionar las conductas más graves que atenten contra el mercado y los derechos de los consumidores, protegiendo así el sistema de formación de precios. Estos delitos se encuentran regulados en el Título XIII del Libro II del Código Penal, bajo la rúbrica «delitos contra el patrimonio y el orden socioeconómico», en el Capítulo XI titulado «De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores», que se estructura en tres secciones. La tercera de estas secciones, que abarca los artículos 278 a 286, se dedica a la regulación de los delitos relacionados con el mercado y los consumidores.

La protección de los consumidores se enmarca dentro del sistema de libre mercado consagrado en el artículo 38 de la Constitución Española, el cual garantiza la libertad de empresa en el marco de una economía de mercado. Sin embargo, el mismo texto constitucional, en su artículo 51, establece que los poderes públicos tienen la obligación de asegurar la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, su seguridad, salud y legítimos intereses económicos. Asimismo, se señala la importancia de promover la información y educación de los consumidores, fomentar sus organizaciones, y escucharlas en las cuestiones que les afecten, todo ello conforme a la ley. Además, se estipula que el comercio interior y el régimen de autorización de productos deben regirse por normativa específica para garantizar la adecuada protección de los consumidores.

Estos principios generales son desarrollados por diversas normas, entre las que destacan la Ley 44/2006, de 29 de di-

ciembre, de mejora de la protección de los consumidores y usuarios, el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios, la Ley 22/2007, de 11 de julio, sobre la comercialización a distancia de servicios financieros destinados a los consumidores, la Ley 29/2006, de 26 de julio, sobre garantías y uso racional de medicamentos y productos sanitarios, la Ley 47/2002, de 19 de diciembre, de reforma de la Ley de Ordenación del Comercio Minorista, la Ley 34/1998, de 11 de noviembre, General de Publicidad, y la Ley 16/2011, de 24 de junio, sobre contratos de crédito al consumo. A estas se suman otras normativas tanto a nivel estatal como autonómico, dado que las Comunidades Autónomas tienen competencias transferidas en esta materia.

En el ámbito europeo, la Recomendación sobre la delincuencia económica, adoptada por el Comité de Ministros del Consejo de Europa el 25 de junio de 1981, insta a la criminalización de diversas infracciones económicas, entre ellas las que afectan a los consumidores, tales como la adulteración de mercancías, la presentación engañosa, las infracciones contra la higiene y la salud pública, y el abuso de la inexperiencia de los consumidores. También aborda la competencia desleal, incluyendo la corrupción de empleados de empresas rivales y la publicidad engañosa. Además, varias directivas europeas buscan armonizar las legislaciones de los Estados en materia de protección de los consumidores, como la Directiva 2009/22/CE, de 23 de abril de 2009, sobre acciones de cesación para la protección de los intereses de los consumidores, la Directiva 2002/65/CE, de 23 de septiembre de 2002, relativa a la comercialización a distancia de servicios financieros, y la Directiva 2005/29/CE, de 11 de mayo de 2005, sobre prácticas comerciales desleales.

La Ley Orgánica 5/2010, de 22 de junio, que modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, expone en su preámbulo las razones para ajustar la normativa en esta materia. Basándose en la Directiva 2003/06 del Consejo, de 28 de enero de 2003, sobre el uso de información privilegiada y la manipulación del mercado, se introdujeron modificacio-

nes en los delitos relativos al mercado y los consumidores. Entre estos cambios, destaca la incorporación de la figura delictiva conocida como «estafa de inversores», que sanciona a los administradores de sociedades emisoras de valores que falseen información para captar inversores o conseguir financiación. Asimismo, se penaliza la difusión de rumores o informaciones falsas con el fin de alterar el precio de cotización de instrumentos financieros, y la realización de operaciones utilizando información privilegiada con el objetivo de manipular la oferta, la demanda o el precio de estos instrumentos.

Finalmente, la Ley Orgánica 1/2015, de 30 de marzo, mantuvo intactas las disposiciones contenidas en el Título XII, centrado en los delitos relativos al mercado y los consumidores. Este conjunto de normativas agrupa una serie de figuras delictivas que, aunque diversas y difícilmente unificables bajo un mismo bien jurídico, protegen el orden socioeconómico, la libertad de competencia y el derecho de los consumidores a recibir productos y servicios de acuerdo con su valor real. Como señala la doctrina, representada por Martínez-Buján Pérez, el bien jurídico tutelado en estos casos es la libertad de competencia, así como el interés de los consumidores en la correcta valoración de los bienes y servicios adquiridos. En cuanto al sujeto activo de estos delitos, salvo que la ley disponga lo contrario, cualquier persona puede serlo, mientras que el sujeto pasivo será aquel titular cuyo interés económico, mercantil o de consumo resulte vulnerado por la conducta ilícita.

2. El bien jurídico protegido en los delitos de revelación de secretos de empresa

La protección de los secretos empresariales encuentra un sólido fundamento en la Constitución Española, específicamente en los artículos 38, 20.1.b) y 33.1. Estos artículos salvaguardan, respectivamente, la libertad de empresa, el derecho a la producción y creación literaria, artística, científica y técnica, así como el derecho a la propiedad privada. Además, como ha sido señalado por una parte de la doctrina, la defensa de los secretos de empresa está intrínsecamente relacionada con el principio de competencia leal o desleal, al referirnos a las acciones que vulneran dichos secretos. Sin embargo, es importante aclarar que la competencia leal no constituye el bien jurídico primordialmente protegido; más bien, es el contexto en el que se debe entender la protección de los secretos empresariales. Finalmente, cabe mencionar que existe una vinculación profunda entre los secretos de empresa y los derechos de propiedad industrial, lo que nos permite avanzar en la precisión del interés jurídico protegido.

Resulta claro que la información que se halla exclusivamente en manos de una empresa es crucial para su desarrollo y su posicionamiento en el mercado. La información confidencial, que puede incluir desde estrategias de negocio hasta datos de clientes, es un activo invaluable. La necesidad de proteger los conocimientos alcanzados por la empresa, tras el desarrollo de una labor de investigación y aportación económica, es la razón básica de la tipificación de aquellas conductas en las que terce-

ros atentan contra la necesidad de preservación de estos secretos empresariales.

La circunstancia de que en muchas ocasiones la empresa pueda ser desconocedora de que ha sido objeto de una conducta lesiva de sus secretos, dada la utilización de discretos medios tecnológicos a la hora de obtener bienes tan inmateriales como secretos o información, hace necesario proteger adecuadamente a la empresa en este ámbito. Los avances tecnológicos han facilitado el acceso no autorizado a información sensible, lo que incrementa el riesgo de que los secretos empresariales sean vulnerados sin que la empresa lo sepa inmediatamente.

Además, ha de ponerse de manifiesto que en aquellas ocasiones en las que una empresa es objeto de tales comportamientos delictivos, se pone de manifiesto públicamente su vulnerabilidad en materia de seguridad, y puede ser una llamada a que se incentive la repetición de tales conductas, dado que se ha puesto de manifiesto la facilidad en el acceso a informaciones secretas. Esta exposición pública no solo afecta la reputación de la empresa, sino que también puede tener consecuencias económicas significativas, ya que los competidores pueden aprovechar esta debilidad para ganar ventaja en el mercado.

Por lo tanto, es esencial que las empresas implementen medidas de seguridad robustas y actualizadas para proteger su información confidencial. Esto incluye la adopción de tecnologías avanzadas de encriptación, la formación continua de los empleados en prácticas de ciberseguridad y la realización de auditorías regulares para identificar y mitigar posibles vulnerabilidades.

A lo largo del tiempo, se han desarrollado numerosas teorías en torno al bien jurídico protegido en estos tipos delictivos, algunas de las cuales han perdido vigencia, como es el caso de las concepciones individualistas centradas en la libertad de la voluntad y aquellas que consideraban el bien jurídico protegido como el derecho patrimonial del empresario titular del secreto. Estas dos corrientes representan las principales teorías surgidas en relación con la naturaleza del secreto empresarial, aunque en la actualidad solo son respaldadas por una minoría.

La primera teoría, centrada en la libertad de voluntad, sostiene que lo que se busca proteger es un derecho de personalidad, específicamente, el deseo de que la información que constituye el secreto no sea divulgada. Esta perspectiva, que se alinea con la teoría subjetiva de la voluntad frente a la teoría del interés, previamente descartada al definir el concepto de secreto empresarial, adquiere relevancia al considerarla en el contexto del ya derogado artículo 499 del Código Penal, que se encontraba en la sección de delitos contra la libertad y la seguridad. No obstante, con la implementación del nuevo Código Penal, la distinción entre secretos personales y secretos empresariales hace inviable esta tesis, ya que, en el caso de los secretos empresariales, la decisión de mantener la confidencialidad está vinculada al avance de la actividad económica, y se enmarca en el principio constitucional de la libertad de empresa. Por lo tanto, se considera más bien un acto de naturaleza económica, dado que la decisión de utilizar o no el conocimiento reservado forma parte integral del plan estratégico de la organización, enfocándose principalmente en los beneficios derivados de la explotación de dichos conocimientos en el ámbito competitivo.

Por otro lado, otro sector doctrinal argumentaba que el delito que penaliza la violación del secreto industrial constituye, en esencia, un ataque contra el derecho de propiedad del titular, bajo una modalidad defraudatoria. Sin embargo, esta tesis es vista como contraria al principio de libertad de mercado consagrado por la Constitución, ya que, de considerarse el bien jurídico protegido como un derecho subjetivo, se estaría otorgando a la empresa una esfera de propiedad exclusiva, capaz de excluir a otros competidores, incluso si estos actúan de buena fe, lo cual contradice los principios de libertad de empresa. Así, cuando se transfiere la información que constituye el secreto, lo que realmente se está cediendo no es un derecho de propiedad, sino los beneficios que se obtienen de su explotación legal[4].

---

4. FERNÁNDEZ SÁNCHEZ, M.T. *Protección Penal del Secreto de Empresa*. Madrid.2000. Pág. 100

Así pues, al transferir la información que constituye el secreto empresarial, lo que realmente se está cediendo no es un derecho de propiedad per se, sino más bien los beneficios que se derivan de su explotación legal.

En este contexto, la doctrina mayoritaria sostiene que, al legislar sobre las conductas relacionadas con el secreto de empresa, lo que se busca proteger es la capacidad competitiva de la empresa en cuestión. En este sentido, BAJO, quien fue pionero en defender esta postura, destaca «La normativa protectora del secreto industrial trata de proteger el interés económico que el secreto encierra para la empresa; ese interés económico se cifra, precisamente en el interés de la empresa en mantener su situación de mercado. El secreto se presenta como un claro valor de empresa, cuyo descubrimiento puede aumentar la capacidad competitiva de los rivales o disminuir la propia capacidad».[5]

La política de confidencialidad adoptada por la empresa tiene como finalidad primordial prevenir que la competencia pueda aprovecharse de los valiosos conocimientos que la organización ha logrado desarrollar. Estos conocimientos, fruto de significativas inversiones y de la acumulación de experiencia, han conferido a la empresa una ventaja competitiva decisiva frente a la mayoría de sus rivales, potenciando su posición en el mercado. En este sentido, el secreto empresarial se erige como un activo patrimonial de incalculable valor para la organización. La revelación de este secreto implicaría un grave perjuicio económico, no solo por la pérdida de la inversión efectuada sino también por el cese de su capacidad para capitalizar exclusivamente estos conocimientos.

En efecto, como bien señala PRATS CANUT, defender esta teoría requiere «situarnos en un ámbito posibilista, toda vez que el objeto último de tutela debería ser la libertad del mercado. No obstante es tal la evidencia de la multiplicidad de factores que

---

5. BAJO FERNÁNDEZ, M. *Derecho penal económico aplicado a la actividad empresarial*, Madrid, 1978. Págs. 286 y ss.

intervienen en el mercado y su configuración que se ha optado en favor de un concepto de libertad limitado, prohibiendo aquellos comportamientos más intolerables, entre los que se encuentra sin duda la competencia desleal, una de sus manifestaciones es justamente la violación de secretos industriales, de tal suerte que la configuración del bien jurídico protegido como la defensa de la capacidad competitiva de la empresa aparece como un objeto de tutela aprehensible y capaz de orientar adecuadamente la interpretación de los distintos tipos penales».[6]

Por otro lado, como recuerda PEDRAZZI al estudiar el bien jurídico en los delitos económicos, en materia de revelación de secretos de empresa se afecta no sólo a bienes jurídicos individuales, como son el patrimonio empresarial en el que se integra ese secreto, sino también bienes jurídicos de naturaleza más colectiva, como la protección de la libertad de empresa y el funcionamiento del mercado (Barbero Santos, 1985)[7]. Esta es una materia en el que se entrecruzan multiplicidad de intereses, empresariales y económicos, y analizarlos nos permite definir más concretamente el bien jurídico protegido en los delitos que estudiamos.

En todo caso, la identificación del bien jurídico protegido en los delitos de revelación de secretos de empresa se ha visto modificado una vez que estos delitos han sido objeto de inclusión en la categoría de «delitos contra el patrimonio y contra el orden socioeconómico». El anterior Código Penal de 1973[8] los había integrado dentro de la categoría de «delitos relativos a la li-

---

6. PRATS CANUT, *Descubrimiento y revelación de secretos de empresa en el Código Penal de 1995*, pp. 182-183.

7. PEDRAZZI, C. *El bien jurídico en los delitos económicos* en BARBERO SANTOS, M. (ed.). La reforma penal: delitos socioeconómicos. Madrid. 1985. Págs. 282-283.

8. Decreto 3096/1973, de 14 de septiembre, por el que se publica el Código Penal, texto refundido conforme a la Ley 44/1971, de 15 de noviembre. «BOE» núm. 297, de 12 de diciembre de 1973, páginas 24004 a 24018 (15 págs.) [Disposición derogada]. Recurso electrónico disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1973-1715

bertad y seguridad», lo que ponía el foco de atención en la figura del empresario y no en la defensa de las informaciones empresariales.

Para poder identificar el bien jurídico protegido es necesario como considera FONT GALÁN, realizar una aproximación a los preceptos contemplados en la Constitución, concretamente aquellos que integran lo que se denomina «Constitución económica» (Font Galán, 1987)[9]. Este término hace referencia al conjunto de principios que deben regir el orden económico, según el constituyente. La aprobación de la Constitución en 1978[10] modificó la concepción que el Código Penal de 1973 tenía sobre los delitos de revelación de secretos empresariales. El hecho de que el constituyente incluyera varios preceptos en la Constitución en los que se reconocía la libertad de empresa y el progreso social y económico motivó que el Código Penal de 1995 introdujera un título denominado «delitos contra el patrimonio y contra el orden socioeconómico», en cuya sección tercera se incluyeron los «delitos relativos al mercado y a los consumidores». Integrada esta sección por los artículos 278 a 280, tal reforma supuso la inclusión de los delitos de revelación de secretos empresariales dentro de los delitos económicos. El cambio de pasar de considerar como delitos relativos a la libertad y seguridad a los delitos de revelación de secretos de empresa, a concebirlos como delitos económicos se produjo como consecuencia de la inclusión de los preceptos constitucionales que fundamentan el orden económico actual. El reconocimiento del derecho a la propiedad privada y a la herencia en el artículo 33 de la Constitución española, del derecho a la libertad de empresa en el marco de una economía de mercado en el artículo 28, la subordinación que el constituyente realiza de toda la riqueza del país al interés general prevista en el artículo 128

9. FONT GALÁN, J. Constitución Económica y Derecho de la Competencia. Madrid. 1987.

10. Constitución Española. «BOE» núm. 311, de 29 de diciembre de 1978, páginas 29313 a 29424 (112 págs.)

o la posibilidad que el Estado se atribuye la función de planificar la actividad económica general contemplada en el artículo 131 motivaron el cambio de rumbo en la conceptualización de los delitos de revelación de secretos empresariales. Y ese cambio de rumbo conllevó una diferente conceptualización de su bien jurídico protegido.

La configuración que la Constitución realiza de nuestro modelo económico, como un sistema basado en la competencia económica, justifica que el legislador, coherentemente con las exigencias del constituyente, proceda a tipificar aquellas conductas que resultan atentatorias contra la economía de mercado y la libre competencia.

En otras palabras, la Constitución establece un marco económico que se fundamenta en la competencia entre las diferentes entidades y actores del mercado. Este enfoque tiene como objetivo principal fomentar un entorno donde las empresas y los individuos puedan competir en igualdad de condiciones, promoviendo así la eficiencia y la innovación.

Para asegurar que este modelo funcione adecuadamente, es necesario que el legislador, siguiendo las directrices marcadas por la Constitución, identifique y regule aquellas acciones que puedan perjudicar el libre funcionamiento del mercado. Esto incluye prácticas como el monopolio, la colusión entre empresas, y cualquier otra conducta que limite la competencia y perjudique a los consumidores.

La tipificación de estas conductas no solo busca proteger el mercado, sino también garantizar que los beneficios de la competencia lleguen a todos los ciudadanos. De esta manera, se promueve un desarrollo económico más justo y equilibrado, donde las oportunidades de crecimiento y éxito no estén restringidas por prácticas desleales o anticompetitivas.

Además, es importante destacar que la intervención del legislador en este ámbito debe ser coherente con los principios y valores establecidos por el constituyente. Esto significa que cualquier regulación o medida adoptada debe respetar los derechos fundamentales y las libertades económicas de los indivi-

duos, asegurando un equilibrio entre la intervención estatal y la autonomía del mercado.

CARRASCO ANDRINO considera que la libertad de empresa puede ser entendida como bien jurídico protegido del delito de revelación de secretos empresariales. Esta libertad, que implica el derecho de cualquier organización empresarial a diseñar su estrategia de planificación y desarrollo en función de los objetivos y recursos económicos, es sin duda alguna uno de los bienes jurídicos que resultan atentados por las conductas tipificadas en el artículo 278 del Código Penal (Carrasco Andrino, 1998).[11]

Tutelar los secretos de empresa supone tutelar la libertad de empresa. Para que se proteja esta libertad es indispensable que la empresa tenga la posibilidad de ejercer sus actividades empresariales sin verse afectada negativamente por conductas lesivas de tal derecho. No es posible ejercer la libertad de empresa sin la información necesaria para que la empresa desarrolle su actividad. Y a su vez, la empresa ejerce su libertad desde el momento en el que decide su forma de organización, los mecanismos de participación en el mercado, la elección y diseño de los bienes y servicios ofrecidos en el mismo, la planificación de sus objetivos económicos, la elección de su nombre, el establecimiento del precio de los productos, o su tipo de clientela.

La jurisprudencia también ha valorado la libertad de empresa como bien jurídico protegido en estos delitos y concretamente la Sentencia del Tribunal Constitucional (en adelante, STC) 88/1986, de 1 de julio afirma que la libertad de empresa conlleva la obligación por parte de los poderes públicos «de evitar aquellas prácticas que pueden afectar o dañar seriamente un elemento tan decisivo en la economía de mercado como la concurrencia entre empresas.[12]

---

11. DEL MAR CARRASCO ANDRINO, M.M. *La protección penal del secreto de empresa*. Madrid. 1998. Págs. 147-148.

12. TRIBUNAL CONSTITUCIONAL. Sentencia del Tribunal Constitucional 88/1986, de 1 de julio. (BOE núm. 174, de 22 de julio de 1986). ECLI:ES:TC:1986:88.

La libertad de empresa favorece la competencia económica y posibilita que las empresas que participan en el mercado lo hagan en condiciones de igualdad y justicia, de manera que su desarrollo se base en el esfuerzo y no en la utilización de técnicas lesivas de la competencia.

El derecho penal ha de actuar contra todas aquellas conductas que lesionen o perjudiquen la libertad de empresa reconocida en el artículo 38 de la Constitución, de manera que, si se actúa infringiendo los criterios de competencia y se accede por medios ilícitos a la información utilizada por una empresa en su libertad y desarrollo económico, el Estado ha de utilizar los medios a su alcance para poner fin a tales situaciones.

También de alguna manera podría entenderse como bien jurídico protegido el derecho de propiedad integrado en el artículo 33 de la Constitución[13]. Todo secreto o información pertenece al empresario y se integra en el patrimonio de la empresa, aunque no tenga una naturaleza material. El patrimonio empresarial no sólo está integrado por los bienes de naturaleza material, sino también por aquellos inmateriales como datos, informaciones o secretos, que son utilizados por la empresa para posicionarse eficazmente en el mercado. La empresa es dueña de tales informaciones y secretos y ha de ser respetada en el ejercicio de su derecho de propiedad, de manera que se vean excluidos actos lesivos o perjudiciales de tal derecho que pongan en peligro la libertad de disposición y uso por parte de la empresa propietaria.

Hay una corriente doctrinal bastante mayoritaria que defiende que el bien jurídico protegido en esta clase de delitos debe ser el derecho de competencia dentro de los términos le-

---

Recurso electrónico disponible en: https://hj.tribunalconstitucional.es/es/Resolucion/Show/651

13. Art 33 Constitución Española «1. Se reconoce el derecho a la propiedad privada y a la herencia. 2. La función social de estos derechos delimitará su contenido, de acuerdo con las leyes. 3. Nadie podrá ser privado de sus bienes y derechos sino por causa justificada de utilidad pública o interés social, mediante la correspondiente indemnización y de conformidad con lo dispuesto por las leyes.»

gales. MUÑOZ CONDE entiende que «el bien jurídico que se protege en este delito es el derecho de competencia leal que hace referencia a los secretos industriales y comerciales legítimamente adquiridos, esto es, la capacidad competitiva de la empresa» (Muñoz Conde, 2023).[14]

Esta visión del bien jurídico enraizado con la competencia nos ha de llevar a analizar la regulación española en materia de competencia desleal. La «Ley 3/1991, de de 10 enero de competencia desleal» en su artículo 13 alude a la revelación o violación de secretos y dispone que «se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales»[15]. La normativa a la que el artículo remite es la «Ley 1/2019, de 20 de febrero de secretos empresariales»[16], que busca la protección de los secretos de empresa por considerarlos indispensables para garantizar el ejercicio de la libertad empresarial. El uso de información y conocimientos en el mercado determina el posicionamiento de una empresa. La utilización de medios ilícitos para alcanzar tal conocimiento, así como la revelación y utilización de los secretos de empresa, suponen una infracción de la libre competitividad y de la economía de mercado. Concebir la libertad de em-

---

14. MUÑOZ CONDE, F. *Derecho Penal. Parte especial.* Valencia. 2023. Pág 158.
15. Ley 3/1991, de 10 de enero, de Competencia Desleal. «BOE» núm. 10, de 11 de enero de 1991, páginas 959 a 962 (4 págs.) Art 13 «1. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14. 2. Tendrán asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo. 3. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto».
16. Ley 1/2019, de 20 de febrero, de Secretos Empresariales. «BOE» núm. 45, de 21 de febrero de 2019, páginas 16713 a 16727 (15 págs.)

presa como bien jurídico en los delitos de revelación de secretos es una consecuencia lógica de la configuración de nuestro modelo económico, pero también ha de considerarse el derecho de competencia como posible bien jurídico afectado por la realización de tales conductas.

De lo he dicho anteriormente puede deducirse que son dos las principales corrientes doctrinales a la hora de configurar el bien jurídico protegido de los delitos de revelación de secretos de empresa. Por un lado, desde una concepción meramente individualista, algunos autores hacen hincapié en el respeto a la libertad de la voluntad del empresario. Por otro lado, ha surgido también una corriente doctrinal que concibe el derecho de propiedad del empresario sobre el secreto como bien jurídico afectado por la comisión del delito.

Sin embargo, podemos entender que tras el Código Penal de 1995 y la consiguiente diferenciación que el texto realizó entre secretos personales y secretos de empresa, parece ser la libertad de empresa el bien jurídico protegido en los delitos objeto de estudio en este trabajo.

Autores como BAJO FERNÁNDEZ entienden que además de la libertad de empresa, estos delitos intentan proteger la capacidad competitiva de ésta (Bajo Fernández M. , 1978).[17]

> «La normativa protectora del secreto industrial trata de proteger el interés económico que el secreto encierra para la empresa. Ese interés económico se cifra precisamente en el interés de la empresa de mantener su situación de mercado. El secreto se presenta como un claro valor de empresa, cuyo descubrimiento puede aumentar la capacidad competitiva de los rivales o disminuir la propia capacidad».

De forma brillante este autor ha identificado el bien jurídico protegido, conceptualizándolo desde una perspectiva económica. Efectivamente la protección de la información tiene por fi-

---

17. BAJO FERNÁNDEZ, M. y BACIGALUPO SAGESSE, S. *Derecho penal económico.* Madrid. 2010. Pág. 288.

nalidad impedir que empresas competidoras adquieran conocimientos que han posibilitado a la empresa cuyos secretos son violados una ventaja competitiva, posicionándola de forma más favorable en el mercado.

El secreto de empresa es un activo más de la misma. Conlleva un valor ineludible dado que su utilización y posesión puede generar importantes beneficios económicos, que, a su vez, conlleven mayores posibilidades de desarrollo e innovación por parte de la empresa.

PRATS CANUTS entiende además necesario mencionar la competencia desleal para la adecuada delimitación del bien jurídico protegido en estos delitos, puesto que considera que «la violación de secretos industriales es una manifestación de competencias desleal». En base a estas consideraciones, el autor entiende que «es la defensa de la capacidad competitiva de la empresa el bien jurídico protegido en estos delitos» (Prats Canut, 1997).[18]

Como decíamos al inicio de este trabajo, las conductas delictivas que estudiamos no sólo atentan contra el interés particular de la empresa o el empresario, sino que viene a perjudicar el interés general de los consumidores y el normal funcionamiento del mercado. Aunque no puede considerarse éste un bien jurídico directamente protegido por el delito, sí pueden considerarse a los consumidores y al mercado como posibles perjudicados por la comisión de estas conductas ilícitas.

La Sentencia del Tribunal Supremo (en adelante, STS) 4811/1964, de 14 de noviembre[19] ya estudiaba en aquellos momentos preconstitucionales las conductas de ofrecimiento y revelación de secretos empresariales como susceptibles de causar un perjuicio para el empresario poseedor de la información afectada. Consideró que «se incluye entre sus derechos el de realizar investigaciones que amparadas sólo por los medios de

---

18. PRATS CANUT, J. *Descubrimiento y revelación de secretos de empresa en el Código Penal de 1995*. Madrid. 1996. Págs. 284 y ss.

19. TRIBUNAL SUPREMO. STS 4811/1964, de 14 de noviembre. ECLI:ES:TS:1964:3123.

legislación sobre propiedad industrial deben permanecer secretas fuera del círculo de empleados y obreros.»

En base a las aportaciones doctrinales y jurisprudenciales analizadas, podemos entender que el bien jurídico protegido es el derecho y el interés de todo empresario en mantener los secretos empresariales ocultos, en base a que su posesión y utilización le reporta beneficios económicos que le permiten diferenciarse de sus competidores. Quizás podríamos hacer una diferenciación entre aquellas conductas de apropiación ilícita de información reservada, que supondría una afectación del derecho del empresario a su libertad y patrimonio, de aquellas conductas que suponen una revelación a terceros o una explotación del secreto, que ya supondría en este caso una afectación del funcionamiento del mercado.

Siguiendo a MORÓN LERMA, parece pues claro que «el bien jurídico protegido es el interés del empresario en el mantenimiento de la reserva», lo que implicará que para la realización del delito se altere de manera efectiva el interés económico del empresario con respecto al secreto violado (Morón Lerma, 2002).[20]

En conclusión, «es el mantenimiento de la reserva lo que proporciona la trascendencia económica que la información asume para su poseedor. Por ello, a nuestro parecer, el bien jurídico protegido se cifra, precisamente, en el interés económico del empresario en el mantenimiento de la reserva».[21] Por lo tanto, la modificación del interés económico del empresario constituirá el requisito esencial exigido para la configuración del delito, teniendo como objetivo primordial la preservación del sistema de competencia en el mercado, el cual se busca proteger a través de esta medida.

---

20. MORÓN LERMA, E. (2002). *La tutela penal del secreto de empresa, desde una teoría general del bien jurídico* [Tesis publicada].Departament de Ciència Política i de Dret Públic, Universitat Autònoma de Barcelona. Reurso electrónico disponible en: https://www.tesisenred.net/bitstream/handle/10803/5066/eml1de5.pdf?sequence=1

21. MORÓN LERMA, E. La tutela penal del secreto de empresa. Op., Cit., Pág. 279.

3. El concepto de secreto empresarial como elemento determinante de la aplicación de los delitos de revelación de secretos empresariales

Antes de adentrarnos en la exploración del concepto jurídico del secreto de empresa, se considera esencial comprender su definición en el ámbito del lenguaje cotidiano. Al dirigir nuestra atención hacia su significado no jurídico, descubrimos que el término «secreto» posee una claridad semántica innegable. De acuerdo con la Real Academia Española secreto se define como «1.Cosa que cuidadosamente se tiene reservada y oculta» «3. Conocimiento que exclusivamente alguien posee de la virtud o propiedades de una cosa o de un procedimiento útil en medicina o en otra ciencia, arte u oficio»[22].

No obstante, en el ámbito de las relaciones jurídicas, al abordar este concepto, se observa una falta de consenso en la literatura jurídica, lo que evidencia la complejidad inherente a su definición. De hecho, uno de los pocos puntos en los que concuerdan los expertos es en la notable dificultad que supone llegar a una definición que sea plenamente satisfactoria.

En la versión anterior del Código Penal, se empleaba el término «secreto industrial» para referirse a la protección de cier-

22. Real Academia Española, «Diccionario de la Lengua Española». Recurso electrónico disponible en: https://www.rae.es/drae2001/secreto

tas informaciones críticas dentro del ámbito empresarial. No obstante, con la promulgación del Código Penal de 1995, se optó por sustituir esta nomenclatura por «secreto empresarial». Este cambio representa un acierto significativo por varias razones:

En primer lugar, porque la Ley de Competencia Desleal, específicamente en su artículo 13, aborda los actos de competencia desleal mencionando expresamente tanto los «secretos industriales» como otros tipos de «secretos empresariales».

Predominantemente, la doctrina sostiene que el concepto de secreto industrial debería ser considerado simplemente como una categoría dentro del más amplio espectro del secreto empresarial. La visión mayoritaria dentro de la doctrina mercantilista argumenta que el secreto empresarial engloba diversos tipos de información que pertenecen a los distintos sectores que componen la actividad empresarial, considerándolos variantes de una misma categoría[23].

Dentro de esta categoría más amplia, el secreto empresarial, se incluyen el secreto industrial y el comercial, con la posibilidad de extenderse a una tercera clasificación. El secreto industrial abarca conocimientos específicos relacionados con la «fabricación de un producto determinado, la aplicación de un procedimiento específico, la producción y oferta de un servicio

---

23. Para determinar el alcance del secreto de empresa, es fundamental prestar atención a la naturaleza de la información contenida en cada una de las categorías que lo integran. Así lo expone FERNÁNDEZ SÁNCHEZ, M.T. *Protección Penal del Secreto de Empresa*, Madrid, 2000. Pp. 45 y ss, donde se distingue entre el secreto industrial y el secreto comercial. El primero abarca las invenciones, los descubrimientos científicos, así como los dibujos y modelos industriales. Por otro lado, el secreto comercial engloba información crítica sobre las preferencias de los consumidores, estrategias de publicidad, estructura de costos y precios, descuentos aplicables, identidad de los proveedores junto con la calidad de sus productos, y los procedimientos de inspección y mantenimiento de la producción a lo largo de todo el proceso de fabricación y comercialización. Además, se incluyen datos sobre la cartera de clientes de la empresa, siempre y cuando dicha información haya sido recopilada tras una inversión significativa de tiempo y recursos, lo que justifica su protección.

particular... y, en general, cualquier dato vinculado al ámbito técnico-productivo de la actividad económica»[24]. Este concepto también comprende los procesos de montaje o reparación, entre otros.

Por otro lado, el secreto comercial se define de manera residual en comparación con el industrial, incluyendo aspectos relacionados con la estructura comercial de la empresa y su organización. Esto implica información sobre la organización interna de la empresa o las relaciones que mantiene con clientes o proveedores.

Adicionalmente, se pueden considerar como parte de los secretos empresariales aquellas informaciones reservadas que conciernen a ciertos aspectos de la organización interna de la empresa, tales como la situación financiera, listas de impagados, contratación de personal cualificado, proyectos de reestructuración interna o externa (incluyendo fusiones, ofertas públicas de adquisición, aumentos de capital, distribución de beneficios o dividendos sociales, entre otros)[25].

Este enfoque más amplio y detallado del concepto de secreto empresarial no solo refleja una evolución en la terminología legal, sino que también proporciona una protección más integral a la diversidad de información valiosa dentro del entorno empresarial, reconociendo su importancia estratégica en el contexto de la competencia desleal y la innovación.

El objeto material de los delitos aquí estudiados es el secreto de empresa, en los términos que se acaba de mencionar. Éste es el término utilizado por la «Ley 3/1991, de 3 de enero de competencia desleal», pero hay otras normas como el «Real Decreto Legislativo 4/2004, de 5 de marzo que aprueba el Texto

---

24. MASSAGUER FUENTES, J.J. *Comentario a la Ley de Competencia Desleal,* Madrid. 1999. pág.385.

25. MORÓN LERMA, E. El Secreto de Empresa: Protección Penal y Retos que plantea ante las nuevas tecnologías, Navarra, 2002, pág.68.

Refundido de la Ley de Impuestos de sociedades»[26] que utiliza el término *know-how*, o la «Ley 30/2007, de 30 de octubre de contratos del sector público» que alude a los «secretos técnicos o comerciales» en el artículo 124[27].

La propia Ley de Secretos Empresariales aludió a esta cuestión en su Exposición de Motivos:

> «Se define el objeto de esta norma como aquella información que sea secreta en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas; tenga un valor comercial por su carácter secreto, y haya sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control. Por consiguiente, esta definición de secreto empresarial no abarca la información de escasa importancia, como tampoco la experiencia y las competencias adquiridas por los trabajadores durante el normal transcurso de su carrera profesional ni la información que es de conocimiento general o fácilmente accesible en los círculos en que normalmente se utilice el tipo de información en cuestión»

---

26. Real Decreto Legislativo 4/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Impuesto sobre Sociedades. «BOE» núm. 61, de 11/03/2004. [Disposición derogada]

27. Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. «BOE» núm. 261, de 31/10/2007. Art. 124 «1. Sin perjuicio de las disposiciones de la presente Ley relativas a la publicidad de la adjudicación y a la información que debe darse a los candidatos y a los licitadores, los órganos de contratación no podrán divulgar la información facilitada por los empresarios que éstos hayan designado como confidencial; este carácter afecta, en particular, a los secretos técnicos o comerciales y a los aspectos confidenciales de las ofertas. 2. El contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato a la que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá durante un plazo de cinco años desde el conocimiento de esa información, salvo que los pliegos o el contrato establezcan un plazo mayor.» [Disposición derogada]

Por tanto, eruditos como CARRASCO ANDRINO han propuesto una dualidad en la conceptualización del secreto empresarial, basada en la inclusión o exclusión de la información correspondiente a la tercera categoría. De esta manera, nos encontramos ante un concepto de secreto empresarial en sentido amplio, el cual abarca cualquier tipo de información sujeta a reserva. Este enfoque es el preferido por la mayoría de la doctrina mercantilista. Por otro lado, existe un concepto en sentido estricto o limitado, que se equipara al término de «know-how», donde se omitiría dicha información.

En el ámbito doctrinal, nos encontramos ante una diversidad de definiciones sobre el secreto empresarial. Entre estas, cabe resaltar la contribución de PRATS CANUT, quien concibe el secreto como «toda información relativa a la empresa, la cual es detentada con criterios de confidencialidad y exclusividad en aras a asegurarse una posición óptima en el mercado frente al resto de empresas competidoras»[28]. Por otro lado, MORÓN LERMA sostiene que «el secreto de empresa comprende toda información relativa a cualquier ámbito, parcela o esfera de la actividad empresarial, cuyo mantenimiento en reserva proporciona a su poseedor una mejora, avance o ventaja competitiva»[29].

De las aportaciones analizadas se infiere, en primer lugar, que la condición de reserva constituye el límite inicial y más evidente al momento de definir el secreto empresarial. En segundo término, se destaca que la naturaleza del secreto empresarial requiere la presencia de múltiples actores: por un lado, el titular y conocedor del secreto, y por otro, aquellos que permanecen ajenos a su contenido. De esta manera, se subraya que una característica esencial del secreto empresarial es su carácter relativo, relegando a la irrelevancia a los denominados «se-

---

28. PRATS CANUT, J.M. *Descubrimiento y revelación de secretos de empresa en el Código Penal de 1995. Delitos relativos a la propiedad industrial, al mercado y a los consumidores*, Madrid, Consejo General del Poder Judicial, 1997, p.184.

29. MORÓN LERMA, La tutela penal del secreto...,Op., cit., p.73

cretos absolutos», es decir, aquellos que no son conocidos por nadie. Esta condición de desconocimiento general contradice el requisito de pluralidad recién demostrado.

En consecuencia, el secreto empresarial se configura a través de una relación específica entre un individuo y un conocimiento determinado. Esta relación implica, por un lado, la emergencia de una obligación para con los sujetos no autorizados de abstenerse de usar o divulgar dicho conocimiento y, por otro lado, confiere al titular la facultad de excluir a terceros de este y decidir sobre su divulgación y explotación. No obstante, es crucial entender que tal facultad no se traduce en un derecho exclusivo, sino más bien en un monopolio de facto que le permite al titular prevenir el acceso ilegítimo de terceros al secreto.

De esta manera, el concepto de secreto se define como «un conocimiento reservado de algo, que da lugar a un status o situación mental determinada. No puede identificarse con lo que sería su mismo objeto. Lo secreto, lo oculto, no son los documentos, cartas, circunstancias, hechos, etc., sino el conocimiento que de ellos se tiene» [30]

Por consiguiente, el secreto puede dividirse en cuanto a su estructura en dos elementos: el objeto, sobre el cual recae el conocimiento que se quiere mantener y el conocimiento que se tiene sobre el mismo. Aunque se utilicen términos como máquinas, documentos o cartas, a tenor del rigor jurídico se exigirá su reforma, aclarando que lo oculto será la actitud mental, no los hechos o cosas.

La jurisprudencia ha intentado conceptualizar también los secretos de empresa. El Tribunal Supremo establece que «No define el CP qué debemos entender por tal, seguramente por tratarse de un concepto lábil, dinámico, no constreñible en un «numerus clausus». Por ello, habremos de ir a una concepción funcional-práctica, debiendo considerar secretos de empresa los propios de la actividad empresarial, que, de ser conocidos

---

30. CARRASCO ANDRINO, M.M. La Protección Penal del Secreto de Empresa, Barcelona, 1998, p. 25

contra la voluntad de la empresa, pueden afectar a su capacidad competitiva».[31]

La AAP Castellón, a 28 de febrero de 2022[32] ha dispuesto que:

> La cuestión fundamental aquí planteada y que gravita parte del recurso es que se ha de entender por secreto de empresa, y como tal puede entenderse cualquier dato que la empresa tenga intención de preservar del conocimiento público, sin que esté necesariamente relacionado con una ventaja competitiva o con un interés exclusivamente económico. Ciertamente, ha de estar relacionado con el tráfico mercantil propio de la actividad de la empresa en cuestión, pues de otro modo no sería calificable de «secreto de empresa», pero fuera de esta especificación el tipo penal no exige ninguna otra.»

El Tribunal Supremo ha hecho otra aportación jurisprudencial en STS 864/2008, 16 de diciembre de 2008[33]

> «Habremos de ir a una concepción funcional-práctica, debiendo considerar secretos de empresa los propios de la actividad empresarial, que, de ser conocidos contra la voluntad de la empresa, pueden afectar a su capacidad competitiva. Así serán notas características: - la confidencialidad (pues se quiere mantener bajo reserva), - la exclusividad (en cuanto propio de una empresa), - el valor económico (ventaja o rentabilidad económica),- licitud (la actividad ha de ser legal para su protección).»

---

31. TRIBUNAL SUPREMO. STS 285/2008 de 12 mayo de 2008.
32. AUDIENCIA PROVINCIAL DE CASTELLÓN. SAP Castellón, 28 de febrero de 2022 - Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039A. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/435fd1c6dfc89317a0a8778d75e36f0d/20231227
33. TRIBUNAL SUPREMO. STS 864/2008, 16 de diciembre de 2008. ECLI:ES:TS:2008:7442. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/ca4dddcef35a60e6/20090219

Sea una u otra la denominación utilizada, lo cierto es que todos estos conceptos hacen referencia a la misma realidad. Y esa realidad no es otra que la información o conocimiento que en el ámbito empresarial es mantenido en reserva y secreto, para evitar que su uso indebido ponga en peligro el posicionamiento de la empresa en el mercado o permita a empresas de la competencia obtener beneficios del secreto ilícitamente conocido.

Es cierto que tradicionalmente la información de carácter reservada que se maneja en el ámbito empresarial ha sido clasificada por la doctrina en dos grupos claramente diferenciados: los secretos de carácter comercial, denominados «secretos comerciales», y aquellos secretos de carácter más técnico o industrial, que suelen recibir la denominación de «secretos industriales». El uso del término secreto empresarial o de empresa, permite por su amplitud, integrar ambos tipos de secretos. La necesidad de utilizar una interpretación extensiva y facilitar la integración en el concepto de secreto de empresa tanto de los secretos comerciales como de los industriales, es defendida por la mayor parte de los autores, destacando principalmente BAJO FERNÁNDEZ, pionero en el tratamiento extensivo del concepto de secreto empresarial.[34]

La AAP Castellón, a 28 de febrero de 2022 - ROJ: AAP CS 2039/2022 hace una clasificación de los secretos de empresa al mencionar que:

> «Su contenido suele entenderse integrado, por los secretos de naturaleza técnico industrial (objeto o giro de empresa); los de orden comercial (como clientela, o marketing) y los organizativos (como las cuestiones laborales, de funcionamiento y planes de la empresa). Y debe 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

34. BAJO FERNÁNDEZ, M. *Derecho penal económico aplicado…*, op cit., Pág. 277.

valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

Por otra parte, la vulneración del secreto de empresa supone un comportamiento desleal previsto también en la Ley 3/1991, de 10 de enero, de Competencia Desleal.»

También el término *know-how*, derivado de la expresión «*knowledge how to do it*», aunque inicialmente fue utilizado para designar a todos aquellos conocimientos necesarios para que pudiera ser utilizada o explotada una invención de forma eficiente, es actualmente un término que «engloba toda aquella información empresarialmente relevante y susceptible de transmisión», en palabras de GÓMEZ SEGADE (Gómez Segade, 1974)[35]. Como consecuencia de la extensión del concepto de secreto de empresa, el término *know-how* actualmente es utilizado como sinónimo de secreto empresarial por la mayor parte de la doctrina como por ejemplo MARTÍNEZ-BUJÁN PÉREZ (Martínez-Buján Pérez, 2010)[36].

Otros autores sin embargo entienden que el concepto de *know-how* es demasiado amplio porque es susceptible de incluir cualquier tipo de información empresarial, incluso aquellos que no tienen carácter secreto, por lo que deberían ser diferenciados ambos conceptos (Carrasco Andrino, 1998)[37].

Las aportaciones del legislador español a la hora de definir el concepto de secreto empresarial se materializaron en los artículos 13 y 14 de la «Ley 3/1991, de 10 de enero, de Competencia Desleal»[38], y los artículos 278-280 del Código Penal. Pero sin du-

---

35. GÓMEZ SEGADE, J. *El secreto industrial. Concepto y protección*. Madrid.1974. Págs. 42-44.

36. MARTÍNEZ-BUJÁN PÉREZ, C. Delitos relativos al secreto de empresa. Valencia. 2010.

37. CARRASCO ANDRINO, M. La protección penal…Op. Cit.,

38. Ley 3/1991, de 10 de enero, de Competencia Desleal. «BOE» núm. 10, de 11/01/1991.Recurso electrónico disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1991-628

da alguna ha sido la «Ley 1/2019, de 20 enero de secretos empresariales»[39] la que ha aportado luz a la hora de definir el concepto. En su artículo 1 ofrece un concepto bastante completo.

> «Artículo 1.
> 1. El objeto de la presente ley es la protección de los secretos empresariales.
> A efectos de esta ley, se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones:
> 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, y
> c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.»

El mismo artículo en su apartado 2 entiende que debe ser considerado «titular de un secreto empresarial cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo».

Por primera vez el legislador ha ofrecido una definición clara de lo que deba entenderse por «secreto profesional», después de las múltiples discusiones doctrinales y jurisprudenciales al respecto. Si bien es cierto que acoge claramente las definiciones que de tal concepto realiza la «Directiva europea 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) con-

39. Ley 1/2019, de 20 enero de secretos empresariales. «BOE» núm. 45, de 21 de febrero de 2019, páginas 16713 a 16727 (15 págs.) Recurso electrónico disponible en:https://www.boe.es/buscar/doc.php?id=BOE-A-2019-2364

tra su obtención, utilización y revelación ilícitas»[40], no podemos desconocer la labor definitoria del legislador.

El hecho de que se haya procedido a la definición del concepto y se haya elaborado una ley explícitamente aplicable a los secretos profesionales es una prueba del interés del legislador en la regulación de la materia. Y este interés deriva lógicamente de la importancia que para la economía y el mercado tiene la gestión de los secretos profesionales. Buscando dar mayor seguridad jurídica y mayor protección a las empresas, sean estas privadas o públicas, la «Ley 1/2019, de 20 de enero de secretos profesionales» constituye un paso indiscutible en la regulación de la materia objeto de estudio en este trabajo. LISTEN ARBEOLA, tras la aprobación de la ley, ha ofrecido un concepto de secreto empresarial concreto y clarificador (Lissén Arbeloa, 2019)[41].

> «El secreto empresarial es un derecho que se proyecta sobre los datos y la información confidenciales de interés para la empresa, susceptibles de atribuir a su titular una ventaja competitiva, no divulgado si siempre que sean objeto de medidas de naturaleza jurídica, técnica u organizativa encaminadas a preservar su carácter secreto».

Acojamos una u otra definición de secreto empresarial, hemos de poner siempre en valor en el carácter eminentemente económico del concepto, puesto que en el caso de los delitos de revelación de secretos de empresa, se busca la protección económica del empresario, que puede verse muy perjudicada en el caso de que los conocimientos o secretos relativos a la

---

40. Directiva europea 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. Recurso electrónico disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016L0943

41. LISSÉN ARBELOA, J. y GUILLÉN MONJE, P. (2019). *Características, alcance de la protección conferida e implicaciones para las empresas en la nueva Ley de Secretos empresariales.* Diario La Ley. ISSN 1989-6913, Nº 9372, 2019.

empresa y que se hallen en su poder, lleguen a ser conocidos por terceros, que los utilicen en su beneficio y en perjuicio de la empresa propietaria de los mismos.

A su vez es necesario que diferenciemos los dos tipos de secretos empresariales más comúnmente admitidos por la doctrina. Por un lado, los «secretos comerciales», que son los explícitamente regulados por la directiva anteriormente mencionada. Son aquellos secretos que contienen información directamente relativa al funcionamiento, naturaleza y organización de la empresa, siendo ésta de tal valor, que se hace necesaria su reserva, imposibilitando que sea conocida por terceros ajenos a la empresa. La razón de su secreto y reserva radica pues en el interés que la competencia tiene en el conocimiento de este tipo de secretos, dado que ponen en riesgo la posición estratégica de la empresa en el mercado.

El segundo tipo de secretos comúnmente admitidos como integrados dentro de lo que se denomina el secreto de empresa, son los «secretos industriales». Estos están integrados por todas aquellas informaciones y conocimientos técnicos e industriales que afectan directamente al diseño y funcionamiento de productos, servicios, estrategias o procesos y que la empresa mantiene en secreto, porque su conocimiento y divulgación puede afectar al valor competitivo de la misma.

Aparte de la labor del legislativo a la hora de definir qué debe entenderse por secreto de empresa, la jurisprudencia ha aportado un concepto amplio, pero a la vez es de destacar la sentencia AAP Vizcaya (Sección 6ª), 235/2005, de 26 de abril, que entiende que «para determinar qué se entiende por secreto de empresa, dicho concepto debe acentuarse en clave objetiva (primando sobre la subjetiva, esto es, la decisión del empresario de considerar «secreto» determinada información) toda vez que es marco de la competencia el interés que subyace en la tutela penal»[42].

---

42. AUDIENCIA PROVINCIAL VIZCAYA. SAP Vizcaya (Sección 6ª), 235/2005, de 26 de abril. ES: APBI:2005:1153. Recurso electrónico disponible en: https://vlex.es/vid/211791523

El tribunal Supremo en la importante STS 864/2008, 16 de diciembre de 2008 considera que

> «Ha de tratarse de un secreto de empresa, concepto más amplio que el de secreto industrial al que se refería el art. 499 de la anterior CP, ya que abarca no solo los relativos a la técnica de los procedimientos de producción, sino también los relativos al comercio u organización del negocio de que se trate.»[43]

Tras este exhaustivo análisis sobre la noción de secreto empresarial, se observa que su definición se caracteriza por una notable amplitud. Esta característica nos lleva a cuestionar si se respetan el principio de legalidad y el mandato de taxatividad en el caso en cuestión.

El principio de legalidad se articula comúnmente mediante la máxima latina «nullum crimen sine previa lege», que se traduce como «No hay delito sin una ley previa que lo establezca como tal». Por lo tanto, una acción solo puede ser considerada delictiva si está expresamente contemplada en la legislación. Este principio salvaguarda contra la posibilidad de acusar y condenar a una persona por un delito de manera arbitraria. Así, de acuerdo con este axioma jurídico fundamental, ningún hecho puede ser tratado como delito sin que exista una ley previa que lo defina de tal manera, incluso si dichos hechos resultan dañinos para el individuo o la sociedad.

Por otro lado, el mandato de taxatividad, que se deriva del principio de tipicidad estricta en el ámbito penal[44], demanda «la definición precisa de los supuestos de hecho de las normas penales». Esta demanda se interpreta generalmente en dos aspec-

---

43. TRIBUNAL SUPREMO. STS 864/2008, de 16 de diciembre de 2008. ES:TS:2008:7442

44. El Artículo 10 C.P establece que «Son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley». Por su parte, según el art. 12 «Las acciones u omisiones imprudentes sólo se castigarán cuando expresamente lo disponga la Ley». Recurso electrónico disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

tos: una disminución de la ambigüedad en los conceptos utilizados para determinar los comportamientos penalmente prohibidos, y una preferencia por el empleo de conceptos descriptivos en lugar de conceptos valorativos[45].

Esto implica que, en aras de la seguridad jurídica, se requiere que tanto los actos y omisiones punibles como las sanciones derivadas de estos sean especificados con exactitud, delimitando el supuesto de hecho de manera estricta y lo más clara posible[46].

En conclusión, al delimitar el concepto de secreto empresarial, se concluye que la descripción del delito o de la situación de riesgo previa al acto delictivo o al comportamiento peligroso es excesivamente amplia. Esto genera una situación de incertidumbre e inseguridad jurídica, lo que conduce al incumplimiento no solo del principio de legalidad, vulnerando así una de las máximas garantías constitucionales[47] y un pilar fundamental del Derecho Penal, sino también del principio de taxatividad que de él emana.

---

45. MORESO, J.J.Principio de Legalidad y causas de justificación (Sobre el alcance de la taxatividad), Doxa: Cuadernos de Filosofía del derecho, Universitat Pompeu Fabra,Barcelona, 2001, pág.527. Recurso electrónico disponible en : http://publicaciones.ua.es/filespubli/pdf/02148678RD28632340.pdf

46. La extensa jurisprudencia del Tribunal Constitucional, tal como se refleja en sus sentencias STC 62/1982, de 15 de octubre, y STC 13/2003, de 28 de enero, establece de manera imperativa este requisito.

47. Art 9 CE art. 9.3, «La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos». Por su parte, el art. 25.1 establece «Nadie puede ser condenado o sancionado por acciones y omisiones que en el momento de producirse no constituyan delito, falta o infracción administrativa, según la legislación vigente en aquel momento». Recurso electrónico disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

4. Características de los secretos de empresa

Una vez definido el concepto de secreto empresarial, resulta imperativo determinar los elementos que, por ende, le confieren valor desde una perspectiva jurídico-penal.

La doctrina alemana ha debatido ampliamente sobre este tema, aunque dicha discusión se considera superada en la actualidad. Este debate se centró principalmente en dos teorías: la teoría de la voluntad o concepción subjetiva (Willestherorie) y la teoría del interés o concepción objetiva (Interessentheorie).

De acuerdo con la teoría de la voluntad, un secreto adquiere relevancia jurídica simplemente con la intención del titular de mantener cierto conocimiento en reserva. Sin embargo, esta perspectiva ha sido criticada por considerarse insuficiente, ya que el contenido y el alcance de la protección jurídica del secreto dependerían exclusivamente de la voluntad del titular. Como señala Carrasco Andrino, esta situación resulta incompatible con los principios fundamentales de un Estado de Derecho, dado que el secreto quedaría definido únicamente por la percepción personal del titular, comprometiendo la seguridad jurídica[48].

Por otro lado, la teoría del interés sugiere que basta con la existencia de un interés valorado positivamente por el ordenamiento jurídico y considerado digno de protección, sin necesi-

48. CARRASCO ANDRINO, La Protección Penal… ,Op., Cit., pág.27

dad de que el titular manifieste explícita o implícitamente su deseo de mantenerlo en secreto. No obstante, esta teoría enfrenta el problema de considerar como secreto empresarial aquella información que, a pesar de ser económicamente relevante para la organización, no es intencionadamente resguardada por su titular.

En consecuencia, se hace evidente la necesidad de adoptar una postura ecléctica que integre de manera equilibrada ambos elementos: la voluntad y el interés. Tal como apunta MORÓN LERMA «la literatura señala que una información constituye secreto empresarial cuando tiene carácter reservado, posee valor competitivo y existe voluntad de mantenerla en secreto por parte de su titular ».[49]

Las características que han de observarse en toda información para que pueda ser definida como secreto de empresa, según la jurisprudencia de los tribunales españoles son las siguientes:

4.1. INFORMACIÓN RELACIONADA CON EL EJERCICIO EMPRESARIAL

La SAP Barcelona 178/2011, 28 de febrero de 2011[50] o la SAP Córdoba 48/2007, 12 de marzo de 2007[51], son algunas de las sentencias que requieren que la información tenga relación directa con la empresa y la actividad por ésta desarrollada para que pueda ser definida como «secreto de empresa».

---

49. MORÓN LERMA, El Secreto de Empresa: Protección…, Op., Cit.,pág. 50

50. SAP Barcelona 178/2011, 28 de febrero de 2011. Roj: SAP B 1349/2011 - ECLI:ES:APB:2011:1349. Id Cendoj: 08019370082011100119. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/f055e9da7f406875/20110505

51. SAP Córdoba 48/2007, 12 de marzo de 2007. Roj: SAP CO 689/2007 - ECLI:ES:APCO:2007:689.Id Cendoj: 14021370032007100180. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/3ae32853e47f2548/20070712

El hecho de que la jurisprudencia exija una relación directa de la información con el ámbito empresarial debería llevarnos a la conclusión de que en aquellas ocasiones en las que la información pertenece a un sujeto no integrado en el ámbito organizativo de una empresa, no sería aplicable la protección penal que el legislador intenta ofrecer a través de la tipificación de los delitos de revelación de secretos de empresa. De hecho, la doctrina entiende que, si el autor de los hechos de acceso, revelación o utilización de secretos empresariales no adopta la forma organizativa propia de una empresa, no sería castigado por la comisión de los hechos descritos en los artículos 278 y siguientes del Código Penal, sino que se acudiría al tipo común del «delito de descubrimiento y revelación de secretos» previsto en los artículos 197 y siguientes del Código Penal. Esta cuestión es clave para delimitar en qué momento resulta aplicable una u otra categoría de delitos.

La necesidad de que la información sea relativa al ámbito empresarial es requerida por la doctrina mayoritaria. GALÁN CORONA explícitamente entiende que

> «la información ha de recaer sobre materias atinentes a la empresa y/ o su actividad. Se trata pues de informaciones relativas a productos, a ideas o procesos de carácter comercial o industrial, y por tanto deberían ser excluidas del término todas aquellas informaciones y datos relativos únicamente a particulares y cuestiones no directamente relacionadas con la empresa» (Galán Corona, 2011).[52]

A nivel de casuística práctica, los límites más bien difusos que rodean al concepto de secreto de empresa, propiciaron situaciones llamativas en las que fueron considerados secretos de empresa los listados de clientes (Auto AAP Barcelona de 20 oc-

---

52. GALÁN CORONA, E. La Regulación contra la Competencia Desleal en la Ley de 10 de Enero de 1991. En A. Bercovitz Rodríguez-Cano, Galán Corona, E.; Quintana Carlo, I. y García-Cruces González, J.A., *Comentarios a la ley de competencia desleal*. Pamplona. 2011. Pág 726

tubre de 2009), los catálogos de productos y novedades (SAP Granada 663/2006, 24 de Octubre de 2006), la estrategia que en cuanto a ventas diseñado la empresa (STS 758/2005, 21 de Octubre de 2005), las estrategias de mercado (STS 758/2005, 21 de Octubre de 2005), la referencias de los productos incorporadas a los catálogos (SAP Granada 72/2007, 2 de Febrero de 2007), etc. A nivel organizativo también se ha concebido como secreto empresarial las partidas contables (AAP Zaragoza 100/2009, 18 de febrero de 2009), los modelos de organización del negocio e incluso los sistemas de promoción interna.

4.2. CARÁCTER SECRETO DE LA INFORMACIÓN

El carácter secreto es un requisito indispensable para poder concebir la información como susceptible de ser calificada como secreto empresarial. Implica que la información no es conocida de forma general por terceros ajenos a la empresa y que claramente no es fácil el acceso ni el conocimiento de la misma por vías legítimas ajenas al marco empresarial.

Desde el punto de vista normativo y a efectos de poder determinar las características que han de concurrir para entender que una información es secreta, nos hemos de remitir al artículo 39.2.a) de la «Directiva UE 2016/943 del Parlamento Europeo y del Consejo de 8 de junio de 2016 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas»[53]. En este precepto se establece que la información ha de ser secreta y «ser secreta en el sentido de no ser,

53. 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 (Texto pertinente a efectos del EEE). Recurso electrónico disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016L0943

en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilicen el tipo de información en cuestión, ni fácilmente accesible por éstas».

Según GÓMEZ SEGADE sólo deberían tener la consideración de «secretos de empresa aquellos cuyo conocimiento se hallan en poder de una o varias personas, mientras que es ignorado por otras». Ello supone que el secreto se encuentra reservado al conocimiento de un círculo muy limitado y concreto de personas (Gómez Segade, 1974).[54]

Para poder determinar si una información es secreta o no, también debería realizarse un juicio de notoriedad, que, analizando las posibilidades de acceso a la información y el número de los legitimados para tal acceso, permitiera concretar si se dan las circunstancias para entender que el secreto no es notorio ni generalmente conocido fuera del ámbito empresarial. SUÑOL LUCEA entiende que este juicio de notoriedad debe realizarse caso por caso, atendiendo a las circunstancias fácticas y a los elementos probatorios que concurran en el supuesto concreto (Suñol Lucea, 2009).[55]

BAJO y BACIGALUPO entienden que un análisis de la doctrina y de la jurisprudencia mayoritaria nos permite afirmar que la información puede seguir siendo considerada secreta a pesar de que fuera conocida por varias de las empresas competidoras en el mismo sector de mercado, si éstas siguen manteniendo el carácter reservado de la información con respecto a los demás competidores (Bajo Fernández M. y., 2010). [56]

No obstante, la postura de la doctrina del Tribunal Supremo es entender que «la información necesariamente ha de estar en poder de su titular legítimo en un régimen de

---

54. GÓMEZ SEGADE, J. *El secreto industrial*...Op. Cit., P. 45.
55. SUÑOL LUCEA, A. *El secreto empresarial. Un estudio del artículo 13 de la Ley de Competencia Desleal.* Madrid. 2009. Pág 271.
56. BAJO FERNÁNDEZ, M. y. *Derecho penal…Op. Cit.,*

exclusividad»[57]. El titular de la información es el interesado en la salvaguardia de su secreto. Pero es plenamente admisible que el secreto sea conocido por terceros y aun así, seguir entendiendo que estamos ante un secreto de empresa y que el titular de éste sigue manteniendo interés legítimo en conservarlo bajo reserva. Si este tercero tiene capacidad para difundirlo y publicitarlo en el mercado, y por tanto hacerlo plenamente accesible a la competencia, sí podríamos entender que la información ya no tiene el carácter de secreta.

En definitiva, aunque el secreto sea conocido por terceros, por parte de empresas competidoras y por trabajadores, la violación de la información contenida en el secreto hace decaer las expectativas de ganancia del titular del mismo. De ahí que resulta justificado tipificar las conductas de revelación y difusión del secreto, aunque aparentemente no parezcan ser capaces de ser reveladas, si ha existido la posibilidad de haber sido conocido por personas diferentes de su titular.

Lo que resulta más relevante para poder determinar si el secreto de empresa lo es o no, son las posibilidades de acceso a la información por parte de los competidores que actual o potencialmente luchan en el mercado dentro del mismo sector con la empresa que ostenta el secreto. El secreto de empresa debe mantenerse protegido del conocimiento de estos competidores pues resulta claro que si acceden al secreto pueden mejorar su posicionamiento en el mercado.

La doctrina entiende que resulta más relevante para determinar el carácter secreto, no tanto el número de personas concretas que tienen conocimiento del secreto, sino si estas personas tienen el carácter de competidores de la empresa cuyo secreto se revela. Otro criterio indispensable para entender que la información tiene carácter secreto es el grado de accesibilidad para personas no incluidas en los círculos empresariales

57. TRIBUNAL SUPREMO. STS 1442/2023, de 20 de octubre. Recurso electrónico disponible en:https://www.poderjudicial.es/search/AN/openDocument/59a051070dcc88f2a0a8778d75e36f0d/20231103

en los que esa información suele ser utilizada. Así, por ejemplo, es posible que los empleados de una empresa, a través de los boletines informativos internos, puedan tener conocimiento de ciertas informaciones por el mero hecho de desarrollar sus actividades laborales en la empresa, pero eso no significa que terceros ajenos a ésta puedan acceder fácilmente al contenido de esa información, dado que no forman parte de la empresa. Habrá de valorarse en todo caso los medios puestos por la empresa para dificultar el acceso a la información, el coste y el esfuerzo empleado para ello. No es necesario que se imposibilite totalmente el acceso, sino que como entiende SUÑOL LUCEA, es suficiente con que se vea dificultado (Suñol Lucea, 2009).[58]

En todo caso, la facilidad para acceder al secreto de empresa depende en gran medida de las medidas adoptadas por el titular del mismo para que no sea conocido por otros competidores o terceros interesados en conocer la información. La cantidad y efectividad de los obstáculos puestos por el empresario para que sus secretos se vean protegidos, deben ser valoradas para poder determinar si el secreto sigue siendo de conocimiento restringido o no. Ello se deduce del tenor literal del artículo 1 de la «Ley 1/2019 de secretos oficiales» que habíamos mencionado anteriormente, en el cual para tener la consideración de secreto empresarial se requiere que la información «haya sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto». Según GÓMEZ SEGADE, estamos ante un elemento de naturaleza subjetiva pues «es el interés del titular del secreto de empresa el que determinará cuál y frente a quien se mantiene secreta» (Gómez Segade, 1974). [59]

El interés del titular de la información tiene, a la vista de la regulación mencionada, una importancia trascendental. La voluntad del empresario en la preservación de la información debe ser manifestada de forma clara, lo que suele materializarse

---

58. SUÑOL LUCEA, A. *El secreto empresarial…Op. Cit.,*Pág. 213.
59. GÓMEZ SEGADE, J. (1974). *El secreto industrial…Op. Cit.,*. Pág. 45

con la adopción de medidas y obstáculos limitativos de un libre conocimiento.

La manifestación de la voluntad de limitar el acceso puede ser expresa. Ello sucedería en el caso de que se adoptaron medidas protectoras como la firma de pactos de confidencialidad o de no competencia. Si el titular del secreto manifiesta expresamente a sus empleados en documentos o en reuniones, que el asunto a tratar es considerado un secreto empresarial, la doctrina y la jurisprudencia mayoritaria entienden que estamos ante una manifestación expresa de la voluntad, porque no se deja lugar a dudas de la intención del empresario de proteger el secreto.

Pero también se considera admisible la exteriorización de la voluntad de forma tácita. Aunque resulta claro que el hecho de adoptar medidas de protección implica que el titular del secreto tiene interés en la preservación de la información, para que la manifestación pueda entenderse producida tácitamente, el establecimiento por ejemplo de contraseñas informáticas para acceder a ordenadores o sistemas de almacenamiento, el uso de cámaras de seguridad en las instalaciones, la limitación a ciertas áreas de la empresa, etc.

Lógicamente surgen menos problemas probatorios en el caso de que la voluntad del mantenimiento del secreto se haya producido de forma expresa. De producirse tácitamente, habrá de hacerse un análisis de las medidas de protección adoptadas, y de la efectividad de estas, lo que puede generar ciertos problemas interpretativos y probatorios en la práctica procesal.

Siguiendo a SUÑOL LUCEA, es acertado recordar que «quien por acción u omisión pone en riesgo su información no puede lícitamente pretender que los demás estén obligados a abstenerse de comunicarla a otros o a utilizarla». Por tanto, si el titular del secreto de empresa no adopta las medidas necesarias para proteger la información que contiene, no podríamos entender cometido un delito de revelación de secretos empresariales.

Corresponde al titular del secreto adoptar las medidas necesarias de protección y actuar con diligencia en su mantenimiento y efectividad. La adopción de las medidas se basa en que el

titular es plenamente consciente de los riesgos que pudieran derivarse del conocimiento generalizado del secreto. Pero si imprudentemente no adoptado las medidas necesarias, no podrá el derecho penal entrar a castigar la conducta de aquellos que acceden o revelan una información que no ha quedado debidamente protegida.

Otra cuestión a tener en cuenta hoy en día es que el titular del secreto de empresa debe ser consciente de los avances tecnológicos y de la facilidad con la que actualmente pueden ser conocidas informaciones empresarialmente relevantes. La utilización de sistemas de almacenamiento masivo y el uso de dispositivos móviles que favorecen la captura de información en periodos reducidos de tiempo, obliga al titular del secreto a adoptar las medidas de autoprotección adecuadas, después de haber valorado los riesgos de acceso y los sistemas de control con los que cuenta la empresa (Faraldo Cabana, 2009).[60]

Si el titular del secreto no adopta tales medidas de protección, no podrá ser posible tipificar las conductas de los que accedan o revelen secretos de empresa obtenidos de manera sencilla por no haber sido debidamente protegidos, con los más mínimos mecanismos tecnológicos de seguridad.

No obstante, esta materia presenta discusiones jurisprudenciales. De hecho, hay algunas sentencias del Tribunal Supremo, entre ellas la STS 864/2008, de 16 de diciembre[61], que conciben que el secreto empresarial puede ser considerado como tal «aunque no haya medidas razonables para proteger el carácter reservado del mismo», siempre que se trate de documentos que indudablemente deben ser considerados reservados. Con lo que parece entender que en ciertas ocasiones el carácter notable-

---

60. FARALDO CABANA, P. *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*. Valencia. 2009. Pág. 235.

61. TRIBUANL SUPREMO. STS 864/2008, 16 de diciembre de 2008. Roj: STS 7442/2008. Recurso disponible en: https://www.poderjudicial.es/search/AN/openDocument/ca4dddcef35a60e6/20090219

mente secreto de los datos o documentos empresariales es de por sí criterio suficiente para requerir de la protección penal.

El Tribunal Supremo no ha sido demasiado exigente en cuanto a la necesidad de adoptar medidas de protección. La STS 285/2008, 12 de mayo[62], ha entendido que para que se hable de secreto de empresa es necesario que se den las notas de «confidencialidad, exclusividad, valor económico y licitud», no considerando tan relevantes las medidas de protección. De la fundamentación jurídica de esta sentencia se deduce que el Supremo no estima indispensable la adopción tales medidas. Debemos criticar esta postura puesto que el derecho penal ha de actuar siempre ante situaciones en las que se atente directamente contra el bien jurídico protegido. Y si ese riesgo de atentado no se obstaculiza con la adopción de medidas de protección, podría entenderse que el titular del secreto de empresa no tiene interés en salvaguardarlo, cuando realmente es todo lo contrario.

4.3. RAZONABILIDAD DE LAS MEDIDAS DE PROTECCIÓN

El legislador español al igual que lo hace la directiva comunitaria en materia de secretos profesionales exige que las medidas adoptadas por el titular del secreto sean razonables. Este es un elemento valorativo que requiere de un análisis de las circunstancias del caso y una adecuada valoración de las mismas.

Para entender que se cumple el criterio de la razonabilidad de las medidas es necesario que el titular del secreto actúe con cuidado y diligencia en el mantenimiento de las medidas de protección. Lógicamente no es necesario que se adopten medi-

62. TRIBUNAL SUPREMO. STS 285/2008, 12 de mayo de 2008. Roj: STS 2885/2008. Recurso disponible en: https://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703

das totalmente infranqueables que imposibiliten totalmente el acceso a la información. La jurisprudencia entiende que es suficiente con que el titular del secreto actúe de forma diligente en la protección del secreto.

Al mismo tiempo para poder entender que las medidas adoptadas son razonables, se requiere que el empresario haya valorado la importancia del secreto a la hora de diseñar las medidas de precaución. En función del valor económico y de uso del secreto y de la consideración de este valor por parte de su titular, será este el que deba adoptar medidas proporcionales a los riesgos de que puedan ser conocidos por terceros. ESTRADA I CUADRAS entiende necesario que se realice siempre «un juicio de riesgo respecto al acceso de terceros» (Estrada i Cuadras, 2016) y en función de los riesgos valorados, se adopten medidas protectoras adecuadas y proporcionadas[63].

Así pues, el juicio de riesgo determinará el tipo y carácter de las medidas a adoptar. Lógicamente aquellas empresas que desarrollan sus actividades en sectores con poca competencia no requieren de medidas extremas, siendo suficiente con la adopción de medidas ordinarias de protección, que puedan considerarse proporcionadas al nivel de riesgo, sin que se le exija a la empresa un esfuerzo desmedido en la protección de la información reservada.

La figura del secreto empresarial presenta, en comparación con otros mecanismos de protección como las patentes, una ventaja fundamental: si se gestiona adecuadamente, permite a su titular mantener un control exclusivo sobre la información, potencialmente de manera indefinida. Esto es así porque el secreto empresarial se fundamenta, como ya se ha mencionado, en el no conocimiento por parte de terceros de la información valiosa, lo que impide que competidores puedan replicar o aprovechar dicho conocimiento en el mercado. A diferencia de las patentes, que otorgan un monopolio legal a cambio de su

---

63. ESTRADA I CUADRAS, A. *Violaciones del secreto empresarial. Un estudio de los ilícitos mercantiles y penales.* Barcelona. 2016. Pág. 118 y ss.

divulgación pública, el secreto empresarial no requiere de tal exposición, lo que le confiere una protección, en principio, más prolongada y potencialmente sin caducidad, siempre que se mantenga la confidencialidad.

Sin embargo, aunque el secreto empresarial ofrece claras ventajas, su protección no es sencilla ni automática. No toda información o conocimiento interno de una empresa puede considerarse un secreto empresarial a efectos legales. De hecho, la jurisprudencia ha dejado claro que la mera naturaleza confidencial o sensible de una información no es suficiente para otorgarle esta categoría. Así lo señala el Tribunal Supremo en su sentencia (Sala de lo Social) nº 1067/2021[64], de 28 de octubre, donde se subraya que «no toda información empresarial, por sensible y confidencial que sea, se considera un secreto empresarial a efectos de la Ley de Secretos Empresariales».

En consecuencia, hay situaciones en las que, a pesar de los esfuerzos invertidos en crear y proteger una información, esta no alcanza la categoría de secreto empresarial. Un ejemplo relevante es la sentencia de la SJM nº 1 de Bilbao nº 20/2022, de 7 de febrero, en la que se declara que «es indiscutible el valor empresarial de la plataforma, pero no es suficiente para considerar que es un 'secreto empresarial' (...) no se concreta qué elementos hacen de esta aplicación algo desconocido para las personas que suelen manejar este tipo de información o de difícil acceso para ellas, como exige el art. 1.1, a, para concluir que el conocimiento es 'secreto'».

Por otra parte, no es suficiente invocar de manera genérica conceptos como el know-how de la compañía. Es esencial precisar qué información en concreto es objeto de protección, para que el tribunal pueda valorar si cumple con los requisitos exigidos por la ley: que sea secreta, que tenga valor comercial y que esté debidamente protegida. Así lo reitera la Audiencia Provincial de Barcelona en su sentencia nº 431/2021, de 12 de mar-

64. TRIBUNAL SUPREMO. STS 1067/2021, de 8 de octubre.

zo[65], al señalar que en la «demanda debe acreditarse de manera clara qué información se considera secreta y si ha sido divulgada o explotada de manera indebida ».

Por todo lo anterior, resulta fundamental que los titulares de un secreto empresarial comprendan la importancia de objetivar qué constituye el secreto, de modo que pueda definirse con precisión y aplicarse las medidas de protección necesarias. En este sentido, no solo es relevante identificar qué información confiere una ventaja competitiva —por no ser conocida por la mayoría de los competidores o por ser de difícil acceso—, sino también implementar mecanismos que aseguren que esa información permanezca resguardada de manera efectiva.

Una vez determinado el secreto empresarial y adoptadas las medidas de protección necesarias, el valor de dicho secreto reside no solo en la posibilidad de explotarlo de manera exclusiva, sino también en la capacidad de transferirlo a cambio de una compensación económica, como sucede con otros activos intangibles.

Una vez clarificada la naturaleza de la información que puede ser considerada secreto empresarial y las medidas necesarias para su protección, el siguiente aspecto a tener en cuenta es cómo defender dicho secreto frente a posibles violaciones por parte de terceros. Uno de los principales desafíos a los que se enfrentan las empresas en este ámbito es el temor a que, al iniciar un procedimiento judicial, la información confidencial se vea expuesta, lo que podría suponer la pérdida definitiva del secreto.

Para mitigar este riesgo, el legislador ha previsto en el Capítulo V de la Ley de Secretos Empresariales una serie de mecanismos destinados a preservar la confidencialidad de los secretos que se revelen en el contexto de un procedimiento judicial. Estos mecanismos incluyen la posibilidad de que el titular del secreto solicite desde las primeras fases del proceso que se declare la confidencialidad de la información y que se adopten

---

65. AUDIENCIA PROVINCIAL. SAP Barcelona 431/2021, de 12 de marzo.

medidas para asegurar su protección (art. 17 LSE), así como diligencias de comprobación de hechos (art. 17 LSE), aseguramiento de pruebas (art. 19 LSE) y medidas cautelares (arts. 20 a 25 LSE).

Además, el artículo 15 de la LSE impone una serie de obligaciones de confidencialidad a todas las partes involucradas en el proceso judicial, incluidos abogados, procuradores, testigos, peritos e incluso el personal de la Administración de Justicia. Estas obligaciones están dirigidas a evitar el uso o divulgación de la información que ha sido declarada como secreta por el tribunal.

> Artículo 15: «1. Las partes, sus abogados o procuradores, el personal de la Administración de Justicia, los testigos, los peritos y cualesquiera otras personas que intervengan en un procedimiento relativo a la violación de un secreto empresarial, o que tengan acceso a documentos obrantes en dicho procedimiento por razón de su cargo o de la función que desempeñan, no podrán utilizar ni revelar aquella información que pueda constituir secreto empresarial y que los jueces o tribunales, de oficio o a petición debidamente motivada de cualquiera de las partes, hayan declarado confidencial y del que hayan tenido conocimiento a raíz de dicha intervención o de dicho acceso.
>
> Esta prohibición estará en vigor incluso tras la conclusión del procedimiento, salvo que por sentencia firme se concluya que la información en cuestión no constituye secreto empresarial o, con el tiempo, pase a ser de conocimiento general o fácilmente accesible en los círculos en que normalmente se utilice».

El tribunal, por su parte, puede adoptar medidas adicionales para proteger la información confidencial, como restringir el acceso a ciertos documentos o limitar el número de personas que pueden asistir a las audiencias públicas y tener acceso a las grabaciones de estas. También se contempla la posibilidad de emitir una versión de la resolución judicial que omita las partes en las que se trate la información secreta, asegurando así su confidencialidad incluso una vez finalizada el procedimiento.

Artículo 15: «2. Los jueces y tribunales podrán, asimismo, de oficio o previa solicitud motivada de una de las partes, adoptar las medidas concretas necesarias para preservar la confidencialidad de la información que pueda constituir secreto empresarial y haya sido aportada a un procedimiento relativo a la violación de secretos empresariales o a un procedimiento de otra clase en el que sea necesaria su consideración para resolver sobre el fondo.

Las medidas a las que se refiere el párrafo anterior podrán incluir, entre otras que sean adecuadas y proporcionadas, las siguientes:

a) Restringir a un número limitado de personas el acceso a cualquier documento, objeto, material, sustancia, fichero electrónico u otro soporte que contenga información que pueda constituir en todo o en parte secreto empresarial;
b) Restringir a un número limitado de personas el acceso a las vistas, cuando en ellas pueda revelarse información que pueda constituir en todo o en parte secreto empresarial, así como el acceso a las grabaciones o transcripciones de estas vistas;
c) Poner a disposición de toda persona que no esté incluida entre el limitado número de personas al que se hace referencia en las letras a) y b) una versión no confidencial de la resolución judicial que se dicte, de la que se hayan eliminado o en la que se hayan ocultado los pasajes que contengan información que pueda constituir secreto empresarial.

La determinación del número de personas al que se hace referencia en las letras a) y b) de este apartado habrá de respetar el derecho de las partes a la tutela judicial efectiva y a un juez imparcial, e incluirá, al menos, una persona física de cada una de las partes y sus respectivos abogados y procuradores.

En todo caso, la adopción, contenido y circunstancias de las medidas para preservar la confidencialidad de la información previstas en este apartado tendrá en cuenta los intereses legíti-

mos de las partes y de los terceros así como el perjuicio que pudiera ocasionárseles, y habrá de respetar el derecho de las partes a la tutela judicial efectiva y a un juez imparcial».

A pesar de estas garantías, el artículo 15 de la LSE aún requiere un mayor desarrollo jurisprudencial. Persisten interrogantes sobre cuestiones clave, como la necesidad de que la información confidencial se destruya tras la finalización del procedimiento, o el régimen sancionador aplicable a quienes incumplan las obligaciones de confidencialidad. También se plantea la duda de si estas medidas de protección deberían extenderse a cualquier tipo de procedimiento judicial que involucre de manera tangencial un secreto empresarial.

No obstante, a pesar de estas incertidumbres, queda claro que el legislador ha hecho un esfuerzo significativo por compatibilizar la protección de los secretos empresariales con las garantías constitucionales del derecho a la tutela judicial efectiva y la imparcialidad judicial.

En definitiva, el secreto empresarial constituye un mecanismo de protección fundamental para las empresas, complementando las herramientas que ofrece la propiedad industrial al preservar el carácter confidencial de aquellos activos intangibles que confieren una ventaja competitiva. Si se cumplen los requisitos establecidos por la LSE, el secreto empresarial adquiere un valor comercial incuestionable. Y, en caso de violación, el marco legal ofrece garantías suficientes para que los tribunales protejan la confidencialidad de la información sin que esta pierda su valor.

Por su parte, la Sala de lo Civil del Tribunal Supremo, en su reciente Sentencia núm. 447/2024, de 3 de abril[66], ha abordado de manera detallada la delimitación del concepto de secreto empresarial, en el contexto de un litigio que involucraba a varios trabajadores que, tras desvincularse de una empresa, hicieron uso de información a la que habían tenido acceso durante su tiempo en ella. Aunque los hechos enjuiciados se rigen por

66. TRIBUNAL SUPREMO. STS 444/2024, de 3 de abril.

la normativa anterior a la Ley 1/2019, de Secretos Empresariales, el Alto Tribunal no ha pasado por alto la legislación vigente en esta materia, integrando su análisis con los principios establecidos por dicha ley.

Un punto de especial interés que se desprende de esta sentencia es la interpretación que el Tribunal Supremo hace del deber de secreto. Según la doctrina sentada por el Tribunal, este deber no puede restringirse exclusivamente a aquellos compromisos contractuales explícitos, como un pacto de confidencialidad, sino que puede existir un deber de secreto implícito, incluso en ausencia de dicho acuerdo escrito. En otras palabras, el deber de confidencialidad puede derivarse de la propia naturaleza de la relación laboral y no está supeditado a la firma de un documento que lo establezca expresamente.

Un ejemplo práctico de esto es el Convenio Colectivo General de la Industria Química (BOE de 9 de abril de 2013), que establece como infracción laboral muy grave la violación del secreto de la correspondencia o de los documentos reservados de la empresa, o la revelación a terceros de datos considerados de reserva obligada. Esta normativa interna sectorial es un claro reflejo de cómo el deber de reserva puede estar estipulado en normas colectivas que trascienden el ámbito individual de los contratos laborales.

No obstante, el Tribunal Supremo subraya que, para que se considere vulnerado el deber de confidencialidad, debe acreditarse que se han divulgado o utilizado indebidamente datos sujetos a reserva obligada. En este sentido, el tribunal deja claro que no puede confundirse el secreto empresarial con los conocimientos generales o específicos que un trabajador o directivo adquiere en el transcurso de su labor profesional y que forman parte de su bagaje profesional, el cual puede utilizar legítimamente en el futuro.

La propia sentencia hace alusión a la razonabilidad de las medidas de protección que se están poniendo de manifiesto a lo largo del presente epígrafe. Así, el Tribunal Supremo, al analizar los hechos del caso, concluye que ni en la primera ni en la segunda instancia se pudo demostrar que la empresa deman-

dante hubiese implementado medidas especiales de protección para salvaguardar la información que consideraba objeto de controversia. Aunque se habían adoptado ciertas medidas de seguridad, como contraseñas, códigos personales y diferentes niveles de acceso a la información, estas eran consideradas como estándar y, por tanto, insuficientes para ser calificadas como razonables a efectos de proteger un verdadero secreto empresarial.

El tribunal especifica que no se exige que las medidas adoptadas sean infalibles, pero es necesario que estas demuestren, de manera clara, que la empresa trataba dicha información como confidencial, reconociendo su valor competitivo. En este caso, la empresa no logró probar que considerara la información como «secreta» o «reservada» de forma inequívoca.

Otro elemento relevante es que no consta en los hechos probados que el empleado hubiera utilizado algún medio específico, como dispositivos o soportes físicos, para sustraer la información. Además, el tribunal consideró que gran parte de la información supuestamente protegida era de dominio común en el sector de siliconas y cauchos, lo que desvirtúa su carácter secreto.

En definitiva, esta sentencia del Tribunal Supremo enfatiza la importancia de que las empresas no solo adopten medidas de seguridad técnicas, sino que también las complementen con políticas claras y efectivas que reflejen la valoración interna de la información como confidencial. Es esencial que se implementen mecanismos que pongan de manifiesto la voluntad de proteger dicha información como un activo estratégico, ya que, en ausencia de estas acciones, se corre el riesgo de que la información no se considere protegida bajo el paraguas del secreto empresarial.

Además, el fallo del Tribunal recuerda que el deber de confidencialidad no se agota con la firma de un contrato de confidencialidad, sino que puede derivarse de la naturaleza misma de la información y su contexto de uso dentro de la organización. Por tanto, para que una empresa pueda invocar con éxito la protección del secreto empresarial en el marco de

un litigio, debe demostrar que ha adoptado medidas proporcionadas y coherentes con el valor estratégico de la información en cuestión.

4.4. VALOR EMPRESARIAL DEL SECRETO

Todo secreto de empresa ha de conllevar ventajas económicas que favorezcan la capacidad competitiva de la empresa. El valor empresarial del secreto viene dado no solamente por su valor de mercado puramente monetario, sino por los beneficios derivados de su uso y aprovechamiento. Además, para que el secreto tenga valor empresarial ha de afectar de forma directa a la actividad desarrollada por la empresa y tener un carácter lícito.

Por lo tanto, la exigencia de que la información empresarial, y por ende, el secreto, tenga valor real o potencial, no representa ningún tipo de dificultad. Todo lo contrario, este valor ha de ser entendido como una ventaja competitiva.

La jurisprudencia ha considerado necesaria, para que un secreto de empresa pueda ser definido como tal, la existencia de un interés en su preservación en orden a favorecer la competitividad y la capacidad de desarrollo de la empresa en el mercado. Así por ejemplo lo considera la SAP Guipúzcoa 22/2007 de 19 de febrero. Es indispensable que exista un interés en la reserva del secreto en tanto en cuanto su difusión o general conocimiento puede favorecer el desarrollo económico y la capacidad competitiva de las demás empresas. La protección del secreto de empresa intenta evitar que las empresas competidoras se beneficien de su conocimiento y causen perjuicios económicos a la empresa titular del secreto.

Podríamos considerar que el valor del secreto radica en la ventaja económica y competitiva para la empresa, y debe ser considerado no sólo desde un punto de vista económico, sino también desde la perspectiva del beneficio que puede derivarse de su utilización. Es lo que suele ser denominado «valor de uso». MORÓN LERMA considera que el que el valor de uso del secreto sea susceptible de generar beneficio durante un periodo

de tiempo limitado no implica que no deba ser considerado como un secreto de empresa. Este autor considera que «el valor de uso es un valor relativo o referencial, que difiere de un titular a otro y que permite a su poseedor actuar estratégicamente y organizar su actividad económica del modo más rentable y beneficioso posible» (Morón Lerma, 2002).[67]

El valor del secreto implica que su posesión redunda en utilidad y beneficio de la empresa. De hecho, a veces no se han tipificado las conductas como constitutivas del delito de revelación de secretos de empresa, cuando el conocimiento de tal secreto no derivaba en ningún tipo de incremento de beneficios, o de utilidad efectiva para la empresa. Algo también avalado por la jurisprudencia que suele entender que en el caso de que la información considerada secreta no aporte ningún tipo de beneficio o utilidad para la actividad profesional desarrollada por la empresa, no puede tener la consideración de secreto de empresa, y en consecuencia, su revelación no puede dar lugar a la estimación de un delito de revelación de secretos empresariales. Para poder determinar si el valor del secreto es de utilidad o no, la jurisprudencia también suele tener en consideración los posibles perjuicios que puedan causarse en el caso de que la información sea conocida, y siendo éstos de notable importancia, sí suele considerar que el secreto es útil y relevante para la actividad empresarial, en tanto en cuanto su revelación protege los intereses en el mercado de la empresa, su volumen de negocio en el mercado y la estabilidad en sus beneficios anuales. Así por ejemplo lo ha entendido la sentencia SAP Barcelona (Sección 8ª), 1036/2002, de 4 de noviembre.

La Ley de Secretos Empresariales establece una clara vinculación entre el valor de la información, entendido como la ventaja competitiva que proporciona, y su naturaleza reservada. Esta conexión puede explicarse a través de tres enfoques o tesis principales, que podemos denominar de la siguiente manera: la tesis de la autonomía condicional del valor empresarial de

---

67. MORÓN LERMA, E. *La tutela penal…Op. Cit.,* Pp. 58-59.

la información, la tesis de la interrelación estricta entre el carácter secreto y el valor de la información, y, finalmente, la tesis de la interrelación relativa entre ambos conceptos[68].

La primera tesis que se puede considerar es la de la autonomía condicional del valor empresarial de la información, que se fundamenta en la idea de que el «valor empresarial» constituye una exigencia que es independiente del carácter secreto de la información, aunque condicionada a ciertos factores. Se considera autónoma en el sentido de que el valor de la información debe existir además de su cualidad de confidencialidad. Tradicionalmente, esta ha sido la tesis dominante en el ámbito jurídico español, como ha sido sostenido por autores destacados como J. A. Gómez Segade, P. Portellano y J. Massaguer, quienes han aportado análisis importantes sobre esta cuestión.

No obstante, esta autonomía del valor es condicional, ya que depende de que la información no pierda su carácter secreto una vez que sea utilizada. Es decir, la información puede tener valor potencial, pero su explotación debe ser cuidadosa para no destruir su confidencialidad, como explica J. Massaguer en su obra sobre la protección jurídica de los secretos empresariales.

No obstante, existen argumentos en contra de la autonomía condicional. En primer lugar, la Ley de Secretos Empresariales no condiciona la protección de la información confidencial al hecho de que su titular efectivamente la explote o tenga la intención de hacerlo. Esto queda claro en el artículo 1.1.d) de la LSE, que establece que el valor empresarial puede ser potencial, lo que implica que la información puede gozar de protección incluso si no ha sido utilizada todavía o, en última instancia, no llega a ser explotada. Por tanto, la protección legal se activa por el simple hecho de que la información posea un valor latente, sin necesidad de uso o implementación efectiva.

En segundo lugar, se debe tener en cuenta el clásico argumento formulado por el economista Kenneth Arrow en su ensayo sobre la transferencia de información. Arrow destacaba la

---

68. https://almacendederecho.org/el-valor-de-un-secreto-empresarial

paradoja inherente a la transmisión de información: el receptor desconoce el valor real de la información hasta que accede a ella, pero una vez que la ha recibido, adquiere el contenido sin coste alguno, salvo que exista un mecanismo legal que proteja al transmisor. Si se adoptara una interpretación demasiado estricta sobre la autonomía del valor empresarial, esto dejaría desprotegidos a inventores, start-ups y otros sujetos que, por falta de recursos, no pueden poner en práctica ideas potencialmente valiosas. En estos casos, los terceros que acceden a dicha información podrían explotarla sin compensación alguna, siempre que argumentaran que dicha explotación hizo que la información dejara de ser secreta.

En tercer lugar, el hecho de que la información pierda su carácter secreto tras ser utilizada no significa que careciera de valor empresarial en el momento previo a su explotación. Existen numerosos ejemplos de información empresarial altamente valiosa, como la relacionada con adquisiciones estratégicas de empresas o la fecha de lanzamiento de un nuevo producto al mercado. A pesar de que esta información deje de ser confidencial una vez divulgada, posee un indiscutible valor comercial antes de ser utilizada y, por ello, debería considerarse susceptible de protección bajo el concepto de secreto empresarial.

Finalmente, determinar de antemano si una información perderá su condición de confidencial tras ser explotada es un juicio prospectivo altamente incierto. Este tipo de análisis, además de complejo, puede ser fácilmente erróneo, ya que la accesibilidad de la información puede variar con el tiempo. Una información que en el presente es de difícil acceso, podría ser más accesible en el futuro debido a la evolución del mercado o de las tecnologías, lo que demuestra la naturaleza volátil del carácter confidencial de la información.

En definitiva, la interpretación que liga el valor empresarial de la información al carácter confidencial de la misma debe manejarse con cautela. La autonomía condicional del valor de la información no puede entenderse como una regla inflexible, ya que el valor puede existir incluso cuando la información aún no ha sido explotada o puede continuar existiendo, aunque la

confidencialidad se vea eventualmente comprometida tras su utilización. Además, cualquier juicio que pretenda predecir la pérdida del carácter secreto es complejo y podría llevar a errores significativos que afecten la protección efectiva de la información. Por ello, es necesario adoptar una visión más matizada y pragmática de la interrelación entre el valor y el carácter secreto, reconociendo que la protección jurídica de la información debe ser suficientemente sólida para evitar que su mera transmisión o explotación la despoje de su valor potencial.

4.5. LICITUD DEL SECRETO

Una cuestión que debemos tener en consideración es si es posible que una información empresarial pueda tener naturaleza ilícita, por propiciar comportamientos o conductas no admitidas por el ordenamiento jurídico, y a su vez ser entendida como secreto y por lo tanto protegida frente a los supuestos de revelación y descubrimiento.

Así, por ejemplo, en aquellas ocasiones en las que las empresas por medios ilícitos obtienen información privilegiada, o cuentan con conocimientos indebidamente obtenidos que les permiten copiar los productos ofrecidos por otras empresas, resulta cuestionable que esa información pueda ser entendida como secreto y por tanto sea susceptible de ser protegida por el ordenamiento, dado que el medio de ser obtenida o su contenido es ilícito.

La cuestión ha obtenido solución a través de la «Directiva 2016/943, del Parlamento Europeo»[69], que ya hemos mencionado a lo largo de trabajo de este trabajo en repetidas ocasiones. En su artículo 5.b establece que «los Estados miembros garanti-

69. 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.

zarán que se deniegue la solicitud de las medidas, procedimientos y recursos previstos en la presente Directiva cuando la presunta obtención, utilización o revelación del secreto comercial haya tenido lugar en cualquiera de las circunstancias siguientes: b) para poner al descubierto alguna falta, irregularidad o actividad ilegal, siempre que la parte demandada actuara en defensa del interés general».

En base a lo dispuesto en este precepto parece claro que es necesario que la información constitutiva de secreto tenga carácter lícito. El precepto mencionado hace referencia a la posibilidad de que aquellos que tengan conocimiento de secretos obtenidos ilícitamente o en los que concurran las circunstancias mencionadas expresamente por el texto, puedan proceder a la denuncia a los efectos de poner de manifiesto las conductas ilícitas cometidas. Es el caso de los denominados *wistleblowers* que han sido normados en el ordenamiento español a través de la «Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción»[70]. De esta norma de reciente aprobación es de destacar lo dispuesto en su artículo 38.5, que para intentar evitar que los denunciantes de infracciones legales cometidas en el seno de una empresa, privada o pública sufran represalias por el mero hecho de haber procedido a la denuncia entiende

> «En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, las personas a que se refiere el artículo 3 de esta ley no incurrirán en responsabilidad de ningún tipo como con-

70. Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. «BOE» núm. 44, de 21/02/2023. Recurso electrónico disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513

> secuencia de comunicaciones o de revelaciones públicas protegidas por la misma. Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de esta ley.»

Entrando más de lleno en la necesidad del carácter lícito del secreto, hemos de señalar que este es un requisito que se considera indispensable por la doctrina para que pueda ser debidamente protegido a nivel penal. La jurisprudencia también es proclive a considerar indispensable la licitud del secreto. De hecho, han sido varias las sentencias del Tribunal Supremo que confirman la necesidad de tal licitud. Concretamente podremos hacer mención a la sentencia del Tribunal Supremo 679/ 2018, de 20 de diciembre[71].

> «El secreto de empresa debe ser definido a partir de una concepción funcional práctica, como los propios de la actividad empresarial, que, de ser conocidos contra la voluntad de la empresa, pueden afectar a su capacidad competitiva. Así serán notas características: la confidencialidad (pues se quiere mantener bajo reserva), la exclusividad (en cuanto propio de una empresa), el valor económico (ventaja o rentabilidad económica), y licitud (la actividad ha de ser legal para su protección).»

La sentencia deja pues totalmente claro la necesidad de que la información que sea objeto de secreto sea ser lícita y legal para poder ser protegida. Además, recuerda expresamente que el concepto de secreto de empresa «es un concepto dinámico,

---

71. TRIBUNAL SUPREMO. STS 679/ 2018, de 20 de diciembre. Roj: STS 4422/2018. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/d0df53eb9917f767/20190118

no susceptible de ser constreñido para una fórmula de *numerus clausus*.

Algunos autores aportan una perspectiva más detallada del asunto. Autores como BAJO FERNÁNDEZ entienden que, aunque en el caso del delito de revelación de secretos del artículo 197 pueden ser protegidas informaciones con contenido ilícito, en el caso concreto de los delitos relacionados con los secretos de empresa, esta ilicitud no sería admisible[72]. Si como hemos visto anteriormente, la finalidad de la protección del secreto radica en la necesidad de garantizar que la empresa actúe lealmente en el ejercicio de su competencia, y dado que en base a esa finalidad no se legitima la utilización de secretos o informaciones para ser utilizadas en beneficio de un tercero, generando situaciones de competencia desleal, no es admisible dar protección a aquellas informaciones que no tengan carácter lícito.

Otra cuestión relativa al valor del secreto es determinar si es indispensable que afecte de forma directa a la actividad de la empresa, o si es suficiente que el secreto tenga un valor potencial de perjudicar en un futuro a la misma, aunque no sea posible apreciar tal perjuicio en el momento efectivo de la revelación. Serían supuestos en los que la actividad empresarial no se ve directamente perjudicada por el conocimiento o la revelación del secreto, pero el hecho de haber obtenido esa información puede ofrecer a aquel que la haya adquirido, la posibilidad de que, en un futuro, adquiera los conocimientos necesarios para obtener beneficios de su uso o explotación.

Por ejemplo, como dice GÓMEZ SEGADE el «conocer que el empresario utiliza materiales de escaso valor para la elaboración del producto» o que, como consecuencia de tales materiales, o de los procedimientos para la elaboración o producción del producto, no cuenta con las mejores características o resulta ineficaz, es una información relevante a efectos de poder subsanar esos defectos y poder obtener una posición prevalente en el mercado, si se alcanza a descubrir la solución al defec-

---

72. BAJO FERNÁNDEZ, M. *Derecho penal económico… Op. Cit.,* P. 287.

to[73]. No cabe duda de que esta información es relevante para la empresa. Si la propia empresa es desconocedora de los defectos de producción, que una tercera empresa pueda conocer los fallos de ésta y ofrecerles solución a los mismos, será una información crucial que devendrá en perjuicio de la empresa afectada si fuera conocida.

En definitiva, lo que se requiere para que la información sea considerada secreto de empresa es afectación económica. La protección jurídica del ordenamiento penal a través de los delitos de revelación de secretos protege todas aquellas informaciones que se puedan considerar relevantes a nivel económico, en tanto en cuanto con su conocimiento se afecta directamente y de forma trascendente a la actividad empresarial. El secreto ha de aportar un valor a la empresa de manera directa, y debe considerarse valioso su posesión y conocimiento.

4.6. LA NECESIDAD DE CUANTIFICAR EL VALOR DEL SECRETO

Mucho se ha escrito en la doctrina sobre la necesidad o no de que el secreto sea valorado en función de los perjuicios económicos que se hubieran ocasionado como consecuencia de su acceso o revelación. Es cierto que el Código Penal al tipificar los delitos de revelación de secretos, no exige expresamente un perjuicio económico concreto para considerar que la conducta pueda integrarse integrada en la definición del delito. Pero es tan relevante la afectación económica que la empresa sufre como consecuencia de la revelación o difusión de sus secretos, que en muchas ocasiones se ha entendido que la cuantía de los perjuicios ocasionados con estas conductas es un elemento relevante a la hora de valorar la información como secreta.

A su vez si tenemos en consideración que la cuantificación de los perjuicios ocasionados será absolutamente indispensable

---

73. GÓMEZ SEGADE, J. *El secreto… Op. Cit.,P. 345*

a la hora de fijar la indemnización por responsabilidad civil, si pudiéramos entender que la cuantificación de los perjuicios es un elemento a tener en consideración para otorgar carácter secreto a la información. Algunos autores han llegado incluso a determinar qué podría entenderse por perjuicios económicos suficientemente graves, llegando a realizar una definición cuantitativa de los mismos, como por ejemplo ESTRADA I CUADRAS, que entiende que «para que una información empresarial secreta merezca las penas previstas en los artículos 278 a 280 lo Penal, debería exigirse al menos que su uso o revelación sean idóneos para causar un perjuicio patrimonial de como mínimo 50.000 euros» (Estrada i Cuadras, 2017)[74]. Resulta muy arriesgado cifrar la gravedad de los perjuicios y hacer depender el carácter secreto de la cuantificación de tal gravedad. Poner cifras específicas supondría limitar la posibilidad de castigar punitivamente aquellas conductas de revelación, que, no causando cuantitativamente tales perjuicios, sí afectan a la empresa de forma directa en su expectativa de beneficios futuros.

Quizás resulta más conveniente el exigir únicamente que las conductas de acceso, revelación o difusión de informaciones empresariales cause un daño inequívoco a la empresa afectada, sin concretar cantidad alguna. Cuantificar este daño puede conllevar sin duda limitar la punición de la conducta. De ahí que podríamos entender que es suficiente con que la empresa se vea perjudicada de forma suficientemente grave, limitando su capacidad competitiva o afectando económicamente a sus beneficios. MORÓN LERMA lo aclara de forma brillante al decir que «la producción del perjuicio se vincula con la pérdida del valor de la información, y, por tanto, con la desaparición de la ventaja de la mejora competitiva que provoca su revelación» (Morón Lerma, 2002)[75]. Con las palabras de este autor queda clara la postura que creemos debe adoptarse, y es la de entender que

74. ESTRADA I CUADRAS, A. El secreto empresarial…Op. Cit., P. 70.

75. MORÓN LERMA, E. *La tutela penal. Op. Cit.,Pág* MORÓN LERMA, E. (2002), La tutela penal del secreto de empresa, desde una teoría general del bien

los perjuicios se consideran relevantes por el hecho de poder afectar a la capacidad competitiva y a los beneficios económicos, independientemente de la cuantía de tales perjuicios.

La posesión de ciertas informaciones relevantes para la empresa constituye sin duda alguna un valor, que es necesario defender y proteger. Con tal finalidad de protección el legislador penal tipifica las conductas de acceso y revelación de tales informaciones, siendo plenamente consciente de que el conocimiento del secreto causa un perjuicio competitivo a la empresa y limita, o a veces incluso imposibilita, su desarrollo en el mercado. Desarrollo que hubiera sido de más fácil obtención en el caso de que el secreto no hubiera sido conocido por terceros competidores. Que los competidores puedan adelantarse a poner en el mercado productos o servicios obtenidos gracias a la información indebidamente sustraída de determinadas empresas, hacen que éstas queden claramente perjudicadas, pues de haber desarrollado debidamente sus conocimientos sin haber sido objeto de una ilícita sustracción de los mismos, ellas habrían sido las destinatarias de los beneficios económicos derivados de la puesta en mercado de esos productos o servicios.

En la mayor parte de las ocasiones la causación de perjuicios se materializa en la pérdida de ventas por parte de la empresa cuyo secreto ha sido divulgado. GÓMEZ SEGADE entiende que para valorar la gravedad de la disminución de las ventas es necesario analizar «las ventas efectuadas antes de entrar en posesión del secreto, el incremento experimentado por consecuencia de la explotación del secreto y la disminución de la cifra de las ventas una vez desvelado el secreto»[76]. Aunque estos tres momentos son claves para poder determinar la entidad de los perjuicios económicos de la empresa afectada, resulta claro que a veces no son claramente cuantificables, sobre todo en aquellas ocasiones en las que la obtención del secreto ha generado un beneficio

---

jurídico, (Tesis Doctoral), Departament de Ciència Política i de Dret Públic, Universitat Autònoma de Barcelona, p.229

76. GÓMEZ SEGADE, J. *El secreto… Op. Cit.,Pág*

para el autor del delito difícilmente valorable dado que está materializado en un producto más efectivo o con unas características prestacionales novedosas, las cuales nunca podría haber alcanzado sin haber estado en posesión del secreto.

Al respecto de la necesidad de protección de secreto empresarial y, por ende, el valor de este, JIMENEZ MURILLO[77] presenta un estudio sobre la protección del secreto empresarial en el mercado interior, analizando la Directiva del Parlamento Europeo y del Consejo del 28 de noviembre de 2013 sobre secretos comerciales.

Destaca que los secretos comerciales, como fórmulas o procesos, no tienen derechos exclusivos como las patentes, pero su divulgación ilegítima puede perjudicar a las empresas. En 2013, el 25% de las empresas de la UE reportaron intentos de robo de secretos, lo que subraya la necesidad de una normativa común para proteger la información empresarial no divulgada.

El concepto de secreto empresarial se define como información no conocida o accesible, que tiene valor comercial y es objeto de medidas razonables para mantenerla en secreto. La protección actual varía entre los Estados miembros, con algunos países careciendo de legislación específica.

La propuesta de directiva busca armonizar la protección de secretos comerciales, estableciendo criterios claros sobre su obtención, uso y divulgación ilícita. Se enfatiza la importancia de proteger la innovación y el desarrollo tecnológico, especialmente para las PYME con recursos limitados.

Las conclusiones resaltan que, aunque la directiva no otorga derechos exclusivos, proteger los secretos empresariales es esencial para fomentar la innovación y el crecimiento en el mercado único de la UE. La propuesta es un paso hacia una protección más robusta y armonizada en toda la Unión Europea.

---

77. JIMÉNEZ MURILO, S. *La necesidad de protección del secreto empresarial en el mercado interior. Salamanca.* 2014

5. Tipo básico del delito de revelación de secretos empresariales. El espionaje industrial

Los delitos de revelación de secretos empresariales están tipificados en el artículo 278 a 280 del Código Penal[78], los cuales se ubican en el Título XIII «delitos contra el patrimonio y contra el orden socioeconómico», Capítulo XI «de los delitos relativos a la propiedad intelectual e industrial, a los mercados y a los consumidores», Sección 3 «de los delitos relativos al mercado y a los consumidores».

El hecho de que los delitos de descubrimiento de secretos se ubiquen dentro de los «delitos contra el patrimonio y orden socioeconómico» es coherente con la afectación de la economía y del mercado, así como la libertad de los empresarios para desarrollar el ejercicio de su actividad dentro de parámetros de libre competencia y lealtad.

El espionaje industrial, esto es, el delito de descubrimiento y revelación de secretos de empresa tiene su punición penal en el artículo 278. Pero hemos de mencionar también la represión que el legislador civil realiza de tales conductas en el artículo 13 de la «Ley 3/1991, de 10 de enero de competencia desleal[79]» al disponer que se considera desleal « la divulgación o explota-

78. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. «BOE» núm. 281, de 24/11/1995.

79. Ley 3/1991, de 10 de enero de competencia desleal. Recurso electrónico disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1991-628

ción, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales», así como « la adquisición de secretos por medio de espionaje o procedimiento análogo».

Mencionemos el tenor literal del artículo 278, en tanto en cuanto ha de ser objeto de un estudio detallado.

> «1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
>
> 2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
>
> 3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.»

Este precepto contempla el tipo básico del delito, y para poder determinar cuándo es aplicable el precepto, por entender que concurren los elementos del tipo, es indispensable realizar un análisis de tales elementos, a efectos de identificar las conductas susceptibles de recibir punición por el legislador penal al considerarse incluidas en el artículo 278.

5.1. SUJETO ACTIVO Y PASIVO DEL DELITO

El artículo 499 del Código Penal, ahora derogado, establecía de manera explícita que únicamente el «encargado, empleado u obrero de una fábrica u otro establecimiento industrial» podía ser considerado sujeto activo del delito, configurándolo, así, como un delito especial propio.

No obstante, la inclusión de la frase «el que» en la reciente normativa penal marca un punto de inflexión hacia la configu-

ración de un delito de carácter general. Esto implica que cualquier individuo que ejecute la conducta descrita en el tipo puede ser considerado sujeto activo del delito, sin la necesidad de poseer atributos o cualidades particulares. Por lo tanto, será suficiente con que la persona lleve a cabo cualquiera de las acciones especificadas en el texto legal, las cuales se procederán a explicar detalladamente a continuación. Este enfoque no solo facilita la adaptación a los avances tecnológicos, sino que también aborda de manera efectiva los riesgos asociados al espionaje informático en el ámbito empresarial.[80]

El delito previsto en el artículo 278 es, por tanto, delito común. No requiere ninguna especificidad en la persona del sujeto activo. Autor puede ser cualquiera, persona física o jurídica, sin que se le requiera condición o característica especial. Sólo se requiere que sea «aquel que no conoce el secreto y que con su conducta trata de acceder o descubrirlo» (Campuzano Laguillo, Palomar Olmedo, & Sanjuán y Muñoz, 2019)[81].

Sin embargo, la doctrina jurídica ha sostenido, con fundamento, que para ser considerado como sujeto activo del delito en cuestión, aunque no se requieren condiciones específicas de manera explícita, es imprescindible la concurrencia de tres condiciones negativas: en primer lugar, que los datos, documentos, soportes u objetos que constituyen el objeto del apoderamiento no le pertenecen; en segundo lugar, que no posee la titularidad sobre los secretos, ya que, de ser así, no actuaría con el propósito de descubrir los secretos de otro, sino que estaría revelando los propios; y, finalmente, que no ha tenido conocimiento de ellos por voluntad expresa de su titular.[82]

---

80. FERNÁNDEZ SÁNCHEZ, M.T. *Protección Penal del Secreto de Empresa*, Madrid, 2000, pp. 230-231

81. CAMPUZANO LAGUILLO, A., Palomar Olmedo, A., & Sanjuán y Muñoz, E. M. *La protección de secretos empresariales*. Valencia. 2019. Pág. 35

82. BAJO FERNÁNDEZ, M. / BACIGALUPO SAGGESE, S.: *Derecho penal económico*. Op. Cit., pág. 532. Los autores citan la STS de 8 de marzo de 1974.

Lógicamente ha de ser aquel que no tengan en su poder los datos, documentos e informaciones que son objeto de sustracción, que a su vez no pueda considerarse titular legítimo de tales informaciones o secretos y que no haya obtenido el acceso o conocimiento del secreto por voluntad del empresario o titular del mismo.

Con respecto a la necesidad de que los datos o documentos donde el secreto se halle no pertenezcan al sustractor, existe jurisprudencia que entiende que las anotaciones realizadas por los trabajadores en libretas de apuntes o cuadernos personales le pertenecen a éstos. Salvo que el empresario haya adoptado medidas de protección para evitar que los trabajadores usen tales métodos, o exista alguna cláusula de confidencialidad que impida a los empleados el traslado de la información empresarial a soportes físicos o informáticos no admitidos por la empresa o soportes no pertenecientes a ésta, puede entenderse que los trabajadores son propietarios de las libretas que contenga la información relevante. Cualquier conducta de utilización, acceso o revelación de los datos contenidos en tales documentos personales no es susceptible de ser tipificada como delito. Por ello y recordando lo que habíamos dicho anteriormente, es siempre importante que el empresario adopte las medidas de protección indispensables para evitar que aquellas informaciones constitutivas de secretos empresariales no sean susceptibles de ser traspasadas a soportes de almacenamiento personales pertenecientes a los empleados.

El empresario también puede utilizar mecanismos de borrado automático o imposibilitar el almacenamiento, o limitar el acceso a la información mediante contraseñas u otros mecanismos restrictivos del acceso. Estos mecanismos serían útiles a nivel de datos almacenados informáticamente. Pero dada la falta de control sobre el acceso a aquellos datos no informatizados, que son conocidos por los trabajadores, y a su vez susceptibles de ser copiados fácilmente en soportes físicos o usando medios tecnológicos de capturas de imágenes o copiado, es indispensable que el empresario manifieste su voluntad de que la información sea tratada como secre-

ta, y a su vez ponga en conocimiento de los trabajadores que en el ejercicio de sus actividades laborales, han de respetar el carácter reservado de los secretos de la empresa, y que para ello, se instala un mecanismo o medida de protección que favorece el sigilo.

Las conductas de aquellos que conociendo de la información en el ejercicio de su actividad laboral y habiéndola traspasado a soportes físicos o tecnológicos, se apropian de tales soportes y tiene un acceso directo y personal a la información, con tal situación de dominio que pueden revelar fácilmente su contenido, podrían ser susceptibles de ser tipificadas en el artículo 279, que castiga la revelación o utilización en provecho propio.

Con respecto a aquellas ocasiones en las que los empleados cesan su actividad laboral, pero continúan teniendo acceso a la información cuando entran en los portales de la empresa utilizando sus propias contraseñas, (contraseñas que pueden estar todavía activas a pesar de que se finalizara la relación laboral, por descuido o dejadez de la empresa), son susceptibles de ser tipificadas en el artículo 279.2, que castiga los casos de utilización en provecho propio.

Podríamos concluir diciendo que por lo que respecta al sujeto activo del delito del artículo 278, puede serlo todo aquel que accede a la información de la empresa de manera totalmente ilícita, no teniendo conocimiento previo sobre tal información.

Respecto al sujeto pasivo en el contexto del delito de revelación de secretos de empresa, existe un consenso significativo dentro de la doctrina jurídica sobre la existencia de una dualidad. Por un lado, se identifica al titular del secreto empresarial, cuyos intereses resultan directamente afectados por la infracción, como la primera víctima directa de la vulneración del bien jurídico protegido. Por otro lado, se considera al mercado en su conjunto como el segundo sujeto pasivo. Esto se debe a que, tal como señala FERNÁNDEZ SÁNCHEZ, el delito atenta contra el correcto funcionamiento de la libre competencia en el mercado, afectando así, de manera amplia, al conjunto de agentes econó-

micos que lo integran[83]. En esta línea, MUÑOZ CONDE sostiene que no solo los individuos pueden ser vistos como sujetos pasivos de estos actos ilícitos, sino que la colectividad en su conjunto también sufre las consecuencias de tales conductas[84].

5.2. CONDUCTA TÍPICA DE APODERAMIENTO

La doctrina jurídica más reconocida ha debatido intensamente sobre el número de modalidades típicas que se desprenden del precepto en cuestión.

En este sentido, el artículo 197.1 del Código Penal, que establece una estructura típica con características específicas, ha sido objeto de análisis por parte de un sector doctrinal que sostiene que dicho artículo contempla tres modalidades típicas.

Estas consisten en: en primer lugar, el apoderamiento de información constitutiva de un secreto de empresa por cualquier medio; en segundo lugar, la utilización de medios o instrumentos específicamente previstos en el artículo 197.1 del Código Penal, lo cual abarca las acciones de interceptación de telecomunicaciones y, por otro lado, el empleo de dispositivos técnicos para la escucha, transmisión, grabación o reproducción de sonido, imagen o cualquier otra señal de comunicación.

Por contraparte, existe otro sector doctrinal que argumenta que el precepto contempla únicamente dos modalidades comisivas: el apoderamiento y el uso de medios técnicos.

Esta última interpretación ha sido la predominante también en el análisis del artículo 278.1 del Código Penal. La utilización de la conjunción disyuntiva «o» para diferenciar estas conductas indica que cada una de ellas puede configurar, por sí sola, la comisión del delito, asignándole a cada una un ámbito típico distinto, configurando así un tipo mixto alternativo.

---

83. FERNÁNDEZ SÁNCHEZ, *Protección Penal…*, Op., Cit., págs.230-231.
84. MUÑOZ CONDE, F., *Cuestiones dogmáticas básicas en los delitos económicos*, Revista Penal, 1998, pág.73.

No obstante, el principal desafío en la interpretación de este tipo penal radica en su redacción, la cual presenta ciertas deficiencias. La inclusión del verbo «apoderarse», tradicionalmente asociado a delitos contra la propiedad material, junto al uso de medios técnicos, introduce una dimensión que se distancia de los delitos tradicionales, generando un campo propicio para interpretaciones divergentes, cada una con sus propios méritos y limitaciones.

El artículo 278.1 requiere el «empleo de los medios o instrumentos señalados en el apartado primero del artículo 197», que son «la interceptación de las telecomunicaciones o la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido de la imagen, o de cualquier otra señal de comunicación».

Resulta claro que el legislador no ha querido poner límites a los medios utilizables para la comisión del delito, toda vez que la cláusula «cualquier otra señal de comunicación» ofrece infinitas formas y métodos de captación de la información, conocidas actualmente o de futura creación.

El tenor literal del artículo 278.1 parece admitir dos tipos de conductas. Aquella que procede al descubrimiento de apoderamiento de secretos «por cualquier medio» y aquel que realiza la conducta «empleando algunos de los medios son instrumentos señalados en el apartado 1 del artículo 197». Analizando las conductas activas que se requieren para la comisión del delito, es necesario descartar la posibilidad de que el mismo pueda ser cometido por comisión por omisión. Añadamos que también la STS 864/2008, 16 de diciembre de 2008 entiende integradas en el tipo estas dos conductas.

> «La acción delictiva consiste alternativamente: a) en el apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos; o b) el empleo de algunos de los medios o instrumentos del apartado 1 del art. 197, el cual, a su vez relaciona unos modos de comisión que aquí no interesa precisar.

> Tal acción delictiva ha de tener por finalidad descubrir un secreto, esto es, algo que conocen una o varias personas que tiene o tienen interés en que no lo conozcan los demás, particularmente los que se dedican a la misma clase de actividad[85].»

Independientemente de cuáles sean los medios utilizados para el apoderamiento, es necesario que éste se haya producido infringiendo las medidas de protección puestas por la empresa a efectos de salvaguardar el carácter secreto que la información.

Es posible que el apoderamiento se realice de forma física, mediante la sustracción de los soportes que contiene la información. Pero dada la utilización preferente y extendida de métodos de almacenamiento informáticos en la actualidad, también podemos entender que la conducta de apoderamiento puede realizarse vía informática. Martín BUJÁN entiende que los datos, aunque no estén recogidos en soportes físicos, deben ser considerados siempre como documentos (Martínez-Buján Pérez, 2010).[86]

Esta interpretación propone una espiritualización del concepto de apoderamiento, que resulta más coherente con la naturaleza etérea del objeto de propiedad en este delito, específicamente el secreto empresarial. Desde este enfoque, se identifica una premisa fundamental en la conducta tipificada por este delito: la captación de un secreto empresarial por parte de un sujeto no autorizado, siendo irrelevante el método empleado para tal fin. Este aspecto depende, en esencia, de la manera en que se manifieste o se divulgue la información en cuestión. Por consiguiente, las diversas modalidades contempladas en la normativa buscan cubrir cualquier vía a través de la cual pueda ser obtenida dicha información.

---

85. TRIBUNAL SUPREMO. STS 864/2008 de 16 de diciembre de 2008. ES:TS:2008:7442

86. MARTÍNEZ-BUJÁN PÉREZ, C. *Delitos relativos al secreto de empresa*. Valencia. 2010. Pág 14

El término «apoderamiento», tal como se establece en el artículo 278.1 del Código Penal, ha experimentado una evolución significativa que se aleja de su interpretación clásica, tradicionalmente vinculada a una dimensión material o física. Este cambio conceptual es evidente en la descripción de conductas delictivas como el robo, definido en el artículo 237 del Código Penal como un acto que afecta a bienes muebles ajenos, y la apropiación indebida, regulada en los artículos 253 y 254, que se refieren específicamente a la posesión indebida de bienes materiales, incluyendo dinero, efectos, valores, o cualquier otro objeto mueble.

Frente a esta perspectiva tradicional, existe un argumento doctrinal bien fundamentado que propone una interpretación de la acción de «apoderarse» que reconozca la naturaleza inmaterial de ciertos bienes, como es el caso del secreto empresarial[87]. Esta interpretación sugiere que habría sido más adecuado emplear términos que connoten una menor materialidad, tales como «hacerse con», «poner a su disposición», «procurarse», «obtener» o «poner bajo su dominio o control». Esta propuesta no solo amplía el espectro de comprensión del término, sino que también implica una reconsideración del resultado del apoderamiento, que no necesariamente conduce a la expropiación o desposesión del bien por parte de su titular.

Esta interpretación ofrece una solución eficaz para superar las deficiencias en la punibilidad que emergían de la postura previa. No obstante, somos conscientes de que esta nueva perspectiva podría enfrentar un desafío significativo, relacionado principalmente con el riesgo de una ampliación excesiva

---

87. Entre otros: MARTÍNEZ-BUJÁN PÉREZ, C.: Delitos relativos al secreto. Op. Cit., págs. 47-48; o MORÓN LERMA, E.: La tutela penal del secreto de empresa. Op. Cit., págs. 533-534, quien afirma que el término «apoderarse» debe ser entendido «como sinónimo de apropiarse, adueñarse, procurarse la información, sin que sea condición indispensable la aprehensión del soporte material que la contiene», incorporando así el tipo conductas de captación mental o intelectual, sin desplazamiento físico, así como apoderamiento físico subrepticio de los objetos que incorporan el secreto.

del concepto de conducta típica. Esto podría llevar a que se considere espionaje cualquier acto de obtención intelectual de información empresarial. Por consiguiente, resulta imprescindible delimitar ciertos límites que restrinjan esta interpretación amplia, antes de determinar qué acciones constituyen casos de relevancia penal y cuáles se encuentran fuera del ámbito de la tipicidad penal.

Volviendo al término apoderarse utilizado por el legislador penal, hemos de acudir a las palabras de Morón Lerma que nos recuerdan que «el término apoderarse debe ser entendido como sinónimo de apropiarse, adueñarse, procurarse la información, sin que sea indispensable la aprensión del soporte material de que la contiene» (Morón Lerma, 2002). Prats Canuts entiende por otro lado que el apoderamiento «no debe vincularse al concepto clásico de apoderamiento físico con desplazamiento de cosa aprehensible, toda vez que el objeto del delito por definición es inmaterial» (Prats Canut, 1997)[88].

La jurisprudencia entiende que el apoderamiento ha de buscar una finalidad y así, la AAP Castellón, a 28 de febrero de 2022 - ROJ: AAP CS 2039/2022, dice que «la voluntariedad de la acción de apoderamiento de los datos tiene precisamente como finalidad la de entrar en conocimiento de ellos».

La conducta de apoderamiento implica la obtención de la información por medios ilícitos. Es indispensable esa ilicitud para que concurra el desvalor de acción que el tipo penal requiere. No cometería la conducta delictiva aquel que usa métodos lícitos o admitidos legalmente. Es necesario que los métodos resulten invasivos, que sean medios indebidamente utilizados y que exista reprochabilidad en la utilización de tales medios para poder entender cometido el delito (Campuzano Laguillo, Palomar Olmedo, & Sanjuán y Muñoz, 2019)[89]. Además, los medios deben ser adecuados para poder eludir los sistemas

88. Idem p.16

89. CAMPUZANO LAGUILLO, A., Palomar Olmedo, A., & Sanjuán y Muñoz, E. M. La … Op. Cit., Pág.39

de protección que el empresario haya establecido para proteger el carácter reservado de la información. Y medios que en consecuencia posibiliten acceder de manera no autorizada al secreto, vulnerando la voluntad de reserva sobre el mismo previamente manifestada por su titular.

En definitiva, el delito de espionaje empresarial se comete por aquel que no estando autorizado accede ilícitamente al secreto, apropiándose de él.

Para aportar mayor luz a las conductas de apoderamiento u obtención de secretos profesionales del artículo 278, creemos que es necesario hacer mención a lo dispuesto en el artículo 3 de la «Ley 1/2019, de 20 de febrero, de Secretos Empresariales»[90] que establece lo siguiente.

> «1. La obtención de secretos empresariales sin consentimiento de su titular se considera ilícita cuando se lleve a cabo mediante:
>
> a) El acceso, apropiación o copia no autorizadas de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes, que contengan el secreto empresarial o a partir de los cuales se pueda deducir; y
>
> b) Cualquier otra actuación que, en las circunstancias del caso, se considere contraria a las prácticas comerciales leales.
>
> 2. La utilización o revelación de un secreto empresarial se consideran ilícitas cuando, sin el consentimiento de su titular, las realice quien haya obtenido el secreto empresarial de forma ilícita, quien haya incumplido un acuerdo de confidencialidad o cualquier otra obligación de no revelar el secreto empresarial, o quien haya incumplido una obligación contractual o de cualquier otra índole que limite la utilización del secreto empresarial.
>
> 3. La obtención, utilización o revelación de un secreto empresarial se consideran asimismo ilícitas cuando la persona que las realice, en el momento de hacerlo, sepa o, en las circunstancias del caso, debiera haber sabido que obtenía el secreto empresarial directa o

90. Ley 1/2019, de 20 de febrero, de Secretos Empresariales. Op. Cit., Recurso electrónico disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-2364

indirectamente de quien lo utilizaba o revelaba de forma ilícita según lo dispuesto en el apartado anterior.»

Así si extrapolamos este precepto al ámbito penal, podemos entender que la «Ley de secretos empresariales» nos ofrece una definición clara de las circunstancias que han de concurrir para que pueda entenderse obtenido o adquirido un secreto empresarial (Fernández Seijo, 2020)[91].

También hemos de recordar que la conducta requiere que el empleo de los medios ilícitos busque la eliminación o la superación de las medidas de protección impuestas para la salvaguarda del secreto. Esto debe llevarnos a pensar que la información que no esté debidamente protegida a través de medidas eficaces y voluntariamente impuestas por el titular del secreto no puede ser entendida como secreto de empresa propiamente dicho, y por tanto no sería punible la conducta de captación que se realizará sobre ella.

En cuanto a cuándo la conducta se considera cometida, PRATS CANUTS entiende que «el artículo 278 se configura como un tipo de peligro que se perfecciona con la realización de la conducta típica de apoderamiento con la intención de descubrir el secreto empresarial»[92].

En todo caso es necesario que el autor haya obtenido de manera efectiva la información empresarial sujeta a reserva, y debemos entender que es indispensable una conducta de apoderamiento, no siendo suficiente el simple acceso. Es cierto que a veces el acceso implica apoderamiento, pues en ciertas ocasiones conocer el secreto conlleva la posibilidad de disponer de él a posteriori, por haberlo retenido mentalmente o por haberlo visto o escuchado. Además del apoderamiento, resulta relevante que mediante la conducta se hayan vulnerado las medidas

91. FERNÁNDEZ SEIJO, J. *Ley de Secretos empresariales. Una aproximación práctica*.Barcelona. 2020 Pág. 14.
92. PRATS CANUT, J. (1997). *Descubrimiento y revelación*…Op. Cit.,.pág. 16.

de protección y como consecuencia, la información reservada haya quedado en poder del autor de los hechos.

Por su arte, el artículo 2 de la Ley 1/2019, de 20 de febrero sobre Secretos Empresariales, aborda los diferentes casos en los que es posible la obtención, utilización y divulgación legítimas de secretos empresariales.

En primer lugar, el artículo 2.1 describe tres situaciones que permiten la obtención lícita de dichos secretos: «a) El descubrimiento o la creación de forma independiente; b) La observación, análisis, desmontaje o prueba de un producto u objeto que haya sido puesto a disposición del público o que se encuentre legalmente en posesión de quien lleva a cabo estas acciones, siempre que no esté sujeto a ninguna obligación que le impida legítimamente obtener la información constitutiva del secreto empresarial; c) El ejercicio del derecho de los trabajadores y sus representantes a ser informados y consultados, de conformidad con la normativa europea o española y las prácticas vigentes».

En segundo lugar, el artículo 2.3 establece diversas situaciones que, aunque inicialmente podrían dar lugar a acciones civiles o penales previstas por la normativa de secretos empresariales, se considerarían lícitas en ciertos contextos: «a) En el ejercicio del derecho a la libertad de expresión e información, tal como se recoge en la Carta de los Derechos Fundamentales de la Unión Europea, incluyendo el respeto a la libertad y pluralismo de los medios de comunicación; b) Con el propósito de revelar, en defensa del interés general, alguna irregularidad, ilegalidad o infracción vinculada al secreto empresarial; c) Cuando los trabajadores informen a sus representantes en el marco del ejercicio legítimo de las funciones que tienen asignadas por la legislación europea o española, siempre que dicha revelación sea necesaria para dicho ejercicio; d) Con el fin de proteger un interés legítimo reconocido por la legislación europea o española. Específicamente, no se podrá invocar la protección de esta ley para obstruir la aplicación de normativas que exijan a los titulares de secretos empresariales divulgar información o comunicarla a las autoridades administrativas o judi-

ciales en el ejercicio de sus funciones, ni para evitar la aplicación de normativas que prevean la divulgación por las autoridades públicas, tanto europeas como españolas, de la información presentada por las empresas que esté en poder de dichas autoridades, en virtud de las obligaciones o prerrogativas conferidas por el derecho europeo o español».

Además de estos escenarios, existen otros dos casos que también permiten la consideración de licitud en la obtención, uso y divulgación de secretos empresariales.

Por un lado, el artículo 2.1.d) establece que la obtención de secretos empresariales será considerada lícita siempre que se realice en el contexto de una práctica comercial honesta. También se contempla la posibilidad de transferencia, cesión o licencia contractual del secreto empresarial. Se entiende que la obtención del secreto empresarial es legítima dado que la naturaleza de este bien jurídico lo hace transferible, tal como lo establece el artículo 4 de la Ley de Secretos Empresariales. No existe ninguna restricción que impida al titular del secreto empresarial cederlo libremente, otorgando al adquirente todos los derechos para su uso en el mercado. No obstante, la normativa también prevé situaciones en las que la utilización del secreto empresarial podría no ser considerada lícita, como la cesión de un secreto empresarial en régimen de cotitularidad por parte de un único propietario (artículo 5 de la Ley 1/2019), así como la responsabilidad que asumiría quien transmita el secreto sin ser titular o sin contar con las facultades necesarias para hacerlo (artículo 7 de la Ley 1/2019) y la posible responsabilidad indemnizatoria del adquirente de buena fe (artículo 9 de la Ley 1/2019).

Por otro lado, más allá de estos supuestos específicos, el artículo 2.2 establece una cláusula general que permite la obtención, uso y divulgación de secretos empresariales siempre que el derecho español o comunitario lo exija o lo permita. Esto puede interpretarse como un refuerzo de los supuestos en los que el interés público o general justifica la revelación de secretos empresariales.

5.3. OBJETO DEL APODERAMIENTO

El artículo 278.1 entiende que la conducta se realiza respecto de «documentos escritos, soportes informáticos u otros objetos que se refieran al secreto de empresa».

El secreto de empresa, como bien inmaterial, suele ser incorporado a medios de almacenamiento informático desde que el uso de las tecnologías se ha generalizado en nuestra sociedad. Por eso debemos entender por «documento escrito» no sólo aquel recogido en soporte material, tal como define documento el artículo 26 del Código Penal que lo define como «todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica», sino que también debemos entender por documento todo aquel soporte informático que contenga datos de semejantes características. Lógicamente como entiende la jurisprudencia no es necesario que el documento sea el original, bastará una simple fotocopia o reproducción de su contenido.

En el caso de que la captación se realice sobre documentos físicos, es necesario que el apoderamiento conlleve un desplazamiento físico de los mismos, sin que en principio parezca suficiente la mera retención o captación intelectual de la información.

FARALDO CABANA nos recuerda que el apoderamiento implica que el secreto quede bajo el dominio del autor y que éste haya sido consciente de haber utilizado medios ilícitos para su obtención, por no tener plena disposición sobre la información[93].

Aparte del apoderamiento físico, es posible el apoderamiento intelectual. Podríamos entender para apoderamiento intelectual de información la memorización de ésta mediante su captación visual o auditiva, sin que sea necesario que la información se incorpore a soportes físicos de almacenamiento o sea trasladada físicamente con intención de apoderamiento.

---

93. FARALDO CABANA, P.. *Las nuevas tecnologías...Op. Cit.,*Pág. 243

Pero, aunque no sea necesario que se utilicen medios de reproducción o almacenamiento, el uso de los mismos no es óbice para la tipificación de las conductas como espionaje empresarial. Tal sería el caso por ejemplo de que se anotaran en un cuaderno datos y secretos.

Cuestión distinta sería el caso de que los datos o informaciones estuvieran a la vista de terceros, sin que concurrieran medidas restrictivas para su acceso. Si una pantalla de ordenador queda abierta, si es posible oír una conversación desde fuera de una habitación o despacho, o si se accede a la información por descuido, y sin voluntad de apoderamiento y acceso como entiende la jurisprudencia, no estamos ante un delito de espionaje empresarial, porque tampoco la información es susceptible de constituir un secreto de empresa. Si está a la vista de todos y no está debidamente protegido, el acceso o el apoderamiento no resultan ilícitos y por tanto no serán castigados penalmente. Que no sea castigado por la vía penal no implica que no pueda obtener castigo por la vía civil, dado que es posible que el empresario acuda a las acciones correspondientes por entender que se trata de un comportamiento contrario a la buena fe comercial del artículo 4.1 de la «Ley 3/1991, de 10 de enero, de Competencia Desleal» (Orts Berenguer, 2001)[94].

El apoderamiento intelectual realizado mediante la memorización de la información no puede dar lugar a un delito de espionaje empresarial salvo que el autor haya infringido las medidas de protección impuestas por el titular de la información, habiendo éste actuado diligentemente en el establecimiento de estas. Es por tanto necesaria que exista diligencia en el empresario a la hora de imponer las medidas de protección.

La jurisprudencia ha analizado supuestos en los que se cuestiona si la conducta pudiera ser considerada como espionaje empresarial o no. Situaciones en las que «la autora accede a parte de las instalaciones de la empresa cuyo acceso está veda-

---

94. ORTS BERENGUER, E. y ROIG TORRES, M. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia. 2001. P. 26.

do, o rebusca en los documentos custodiados por el empresario en sus cajones o archivadores», como ha analizado la STS 446/2001 de 21 de marzo, o accede sin permiso al despacho del empresario, o se oculta en un lugar apartado para poder obtener la información Estos son supuestos en los que la doctrina ha entendido, que en tanto en cuanto el secreto ha sido vulnerado y extraído de la esfera del empresario de manera ilícita, las conductas deberían ser castigadas en todo caso como un delito de espionaje empresarial del artículo 278 (Fernández Sánchez, 2000)[95].

Una materia por analizar es lo que debamos entender por datos, y si pueden ser considerados como tales el conocimiento de palabras clave o elementos que permitan conocer el contenido del dato, aunque no se haya tenido acceso directo al mismo. Es lo que suele denominarse metadatos. Un ejemplo son los asuntos de los correos electrónicos o el título de los mensajes. Resulta claro que muchas veces el conocimiento del asunto del email, sin llegar a conocer o acceder al cuerpo del texto, conlleva ya de por sí un conocimiento del secreto.

El título de un email o mensaje suele ser indicativo de la información que en él se contiene y si esta información fuera reservada, bastaría su lectura para alcanzar su conocimiento. En estos casos la jurisprudencia y la doctrina suele entender que cuando esos metadatos se obtienen de una cuenta de correo electrónico o de un teléfono, dado que estos dispositivos cuentan con contraseñas y mecanismos de limitación para su acceso, resultaría claro que las conductas de acceso y apoderamiento serían susceptibles de ser punidas por la vía del artículo 278. En cambio, en aquellas ocasiones en las cuales se publican ciertos documentos a nivel de la empresa, en su web, *newsletter*, etc, que incluyen esos metadatos, o cuando el título de estos revela información empresarial, ésta no puede ser entendida como secreto porque no se observa en el empresario una vo-

---

95. FERNÁNDEZ SÁNCHEZ, M. *Protección penal del secreto de empresa*. Madrid.2000. Pág 229.

luntad de restringir su acceso. La publicación en webs internas implica una falta absoluta de medios de protección de la información en cuestión (Fernández Sánchez, 2000).

Por otro lado, en aquellas ocasiones en las cuales los datos están incorporados a medios o sistemas informáticos, si el autor procede a la copia de los datos, o los reproduce de manera que adquiere su conocimiento, hemos de entender que se ha consumado el apoderamiento. Sobre esta cuestión ha ahondado MORÓN LERMA que entiende que «cuando la grabación del documento registrado en cualquiera de las memorias electrónicas del ordenador al disquete se produzca directa y materialmente por el sujeto, esto es, no a distancia por medio de la conexión del ordenador vía módem a la red telefónica», la conducta podría ser susceptible de no merecer reprochabilidad penal, porque el autor considera que «si la conexión se produce telemáticamente, la conducta quedaría subsumida en la modalidad típica relativa a la interceptación o control ilícito de señales de comunicación» (Morón Lerma, 2002)[96].

No obstante, lo más frecuente es que si los datos están incorporados a medios informáticos, sea necesaria una reproducción para la obtención de la información. En estos casos el apoderamiento implica una conducta activa por parte del autor, a efectos de poder asegurarse el apoderamiento. Resulta lógico que si los datos, por su extensión y complejidad, se incorporan a medios de almacenamiento tecnológico, el autor de los hechos no podrá proceder a su memorización, o captación intelectual de forma momentánea. Requerirá la utilización de mecanismos de reproducción y captación de los datos y por tanto esta conducta activa será necesaria para entender que el delito se comete. Acceder a un sistema informático y conocer datos que por su complejidad o extensión no puedan ser memorizados, no debería dar lugar a la aplicabilidad del delito de espionaje industrial, porque sería imposible su uso y aprovechamiento posterior.

---

96. MORÓN LERMA, E. La tutela penal del secreto de empresa…op, cit. Pág.

CASTRO MORENO considera que no se debería hacer diferenciación entre apropiarse del soporte informático, realizar una copia de los datos en un soporte similar o enviar la información a través de la nube o mecanismos similares. De hecho, expresamente tiende a recalcar que «se apodera del secreto de empresa en el sentido típico, no sólo quien se lleva un documento escrito a un disquete informático que contiene los datos secretos, sino también quien, sin aprehender estos soportes materiales, reproduce o copia en otros documentos o soportes los datos contenidos en aquellas» (Castro Moreno, 2006)[97].

La ya mencionada «Directiva UE 2016/943» establece en su artículo 4.2 lo siguiente.

> «2. La obtención de un secreto comercial sin el consentimiento de su poseedor se considerará ilícita cuando se lleve a cabo mediante:
>
> a) el acceso no autorizado a, así como la apropiación o la copia no autorizadas de, cualquier documento, objeto, material, sustancia o fichero electrónico, que se encuentre legítimamente bajo el control del poseedor del secreto comercial y que contenga el secreto comercial o a partir del cual este se pueda deducir;
>
> b) cualquier otro comportamiento que, en las circunstancias del caso, se considere contrario a unas prácticas comerciales leales.»

Del precepto parece deducirse que la reproducción conlleva apoderamiento, y que realizar una copia de los ficheros electrónicos implica la comisión del delito de revelación de secretos de empresa. Y ello será así siempre y cuando el acceso se haya realizado ilícitamente, lo que sucede cuando se haya accedido sin permiso a los dispositivos que contenían la información, siendo el autor consciente de su falta de autorización para el acceso.

---

97. CASTRO MORENO, A. *El Derecho penal español ante el espionaje industrial y el secreto de empresa* (artículos 278 a 280 CP). *Rivista Trimestrale di Diritto penale dell'Economia*. 2006.

Habíamos considerado anteriormente que la obtención de la información que aparece en una pantalla de ordenador abierta, o en los papeles colocados encima de una mesa a la vista de terceros no podía ser considerada secreto por no haber sido debidamente protegida. Pero si existe por parte del autor un deber con la empresa en base a un pacto de confidencialidad, la conducta sí sería susceptible de ser castigada. Y posiblemente el tipo penal que más encajaría sería el supuesto el artículo 279.

El acceso a los datos puede también realizarse de forma remota, accediendo telemáticamente y sin necesidad de contacto físico con el soporte que contiene los datos. Esta posibilidad ha estado prevista por el legislador en la redacción del texto del artículo 278, dando cabida a la utilización de los «medios contemplados en el artículo 197. 1 del Código Penal» y permitiendo que el ciberespionaje sea castigado en nuestro ordenamiento jurídico.

El «Instrumento de ratificación del Convenio sobre la ciberdelincuencia, hecho en Budapest el 23 noviembre de 2001»[98], es el primer texto normativo europeo que trata la materia. Concretamente el artículo 3 relativo a la interceptación ilícita establece que:

> «Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.»

---

98. Instrumento de ratificación del Convenio sobre la ciberdelincuencia, hecho en Budapest el 23 noviembre de 2001. «BOE» núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896 (50 págs.) Recurso electrónico disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

De la redacción se desprende que la ilicitud de la interceptación de datos o informaciones mediante la utilización de medios técnicos «es posible que se realice sobre las comunicaciones entre un sistema informático y otro, y sobre las informaciones que están dentro del sistema» (González Cussac, 2013)[99].

Puede suceder también que se haya accedido a los sistemas informáticos que presuntamente contenían información secreta, pero sin alcanzar el éxito en el descubrimiento de la información. En estos casos lo punible sigue siendo el acceso, independientemente de que por cualquier motivo la información secreta no haya sido conocida.

La interceptación debe ser contemplada, a la luz de la redacción amplia por parte del legislador, como susceptible de abarcar toda acción de obtener información empresarial reservada almacenada en medios tecnológicos o comunicada de manera telemática, mediante el uso de medios informáticos que permiten el acceso ilícitamente usando redes de telecomunicación. Las conductas de interceptación tecnológica son mucho más frecuentes actualmente, dado que la práctica totalidad de las empresas cuentan con el almacenamiento de sus datos e informaciones en sistemas informáticos, aparte de ser ya muy común el uso de Internet para las comunicaciones e intercambio de archivos. También sería posible que las informaciones secretas estuvieran contenidas en las redes internas de la empresa, como sucedería en el caso del almacenamiento o archivo por intranet.

El uso generalizado de sistemas de almacenamiento a través de la nube, u otros servicios privados de gestión de archivos por parte de las empresas conlleva una mayor probabilidad de que los datos contenidos en ella sean conocidos por terceros. De ahí que es necesario que el empresario adopte todas las me-

---

99. GONZÁLEZ CUSSAC, J. *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*. Valencia. 2013. Pp. 173-174

didas de protección indispensables para evitar situaciones de ciberataques o riesgos de obtención de datos por parte de hackers. Ha de recordarse también que existen programas maliciosos que penetran en el sistema informático de una empresa, accediendo a la información de manera remota. Estas conductas son constitutivas también de interceptación telemática y susceptibles de ser castigadas penalmente. Si mediante la utilización de estos sistemas de hackeo se accede de manera ilícita a la información, estaríamos ante una conducta susceptible de ser subsumida en la vía del artículo 197 bis. Pero si como consecuencia del acceso, el autor se apropia del secreto, utilizándolo de manera que se merme los derechos del empresario sobre el mismo, estaremos ante un supuesto de espionaje empresarial del artículo 278.

Si algo puede deducirse del tipo básico contemplado en el artículo 278 es la voluntad del legislador de incluir «cualquier medio de comunicación o telemático». Esta es una garantía de que la aparición en un futuro de medios de captación u obtención de la información quedará incluida dentro de la redacción amplia ofrecida por el legislador, con lo que existen claras garantías de que el secreto de empresa quede protegido, a pesar del futuro desarrollo de la tecnología. Pero también es cierto que hay jurisprudencia que entiende innecesaria la remisión a los medios del artículo 197.1, como AAP Castellón, a 28 de febrero de 2022[100], por considerarla redundante.

---

100. AAP Castellón, a 28 de febrero de 2022. Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039A. Id Cendoj: 12040370022022200755. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/435fd1c6dfc89317a0a8778d75e36f0d/20231227

5.4. ÍTER CRÍMENES Y FORMAS IMPERFECTAS DE EJECUCIÓN DEL DELITO

El tipo básico del artículo 278.1 constituye un delito de resultado, que considera insuficiente el apoderamiento para entender consumado el delito. Es indispensable para que se entienda consumado que se haya producido además una afectación del bien jurídico protegido, que recordemos era preservar las facultades de exclusividad y propiedad que corresponden al empresario sobre los secretos de la empresa, pues resulta claro que cualquier acceso o apropiación indebida de los datos afecta a sus capacidades competitivas. La consumación conlleva que el secreto quede bajo el control del autor que ha procedido al apoderamiento.

El exigir para la consumación el apoderamiento efectivo implica que el autor pone bajo su poder el secreto, de manera que tiene posibilidad de utilizarlo a posteriori y disponer de él quedando bajo su poder, aunque no es necesario que lo haya utilizado o que haya obtenido ventaja económica derivada de su uso o explotación.

Dado el carácter inmaterial de los secretos de empresa y la generalización y actual accesibilidad de medios tecnológicos para el apoderamiento, suele ser frecuente que éste se produzca y sin embargo no suponga que el empresario deje de estar en posesión del secreto. Parte de la doctrina entiende que, si como consecuencia del apoderamiento también se priva de la posesión al titular del mismo, estaríamos ante un supuesto de concurso de delitos.

En cuanto a las formas imperfectas de ejecución en los supuestos del artículo 278.1, son admitidas por la jurisprudencia y se producen en aquellas ocasiones en las que se haya intentado el apoderamiento o la interceptación, pero no se haya conseguido. En los casos de interceptación de las comunicaciones, parte de la doctrina entiende que es suficiente la colocación de mecanismos de captación, micrófonos, cámaras o dispositivos similares. Pero lo cierto es que el uso de estos mecanismos, si finalmente no se llega a producir la captación o grabación de

imágenes o audio, no daría lugar a un delito de descubrimiento y revelación de secretos empresariales, porque no podría entenderse consumado el delito. Esa falta de consumación se debe no sólo a la ausencia o imposibilidad de obtención de la información secreta, sino al hecho de que ésta en ningún momento ha estado en poder de dominio por parte del autor de los hechos.

Cuestión distinta es la conducta de mera utilización de artificios de escucha o grabación de imagen. En estos casos el legislador entiende que la mera utilización de tales dispositivos es sancionable penalmente, independientemente de que con ellos se haya obtenido un resultado de captación o utilización de estos o no.

Como se establece en la sentencia SAP Valencia 2961/2022 de 16 septiembre de 2022[101], citando la sentencia 222/2020, de 17 de la Audiencia Provincial de Madrid «estamos ante un delito de peligro concreto, desde la perspectiva del bien jurídico protegido, que se consuma por el medio apoderamiento o empleo de los artificios con intención de descubrir, consumación anticipada, siendo indiferente que el sujeto activo llegue a descubrir el secreto».

Una de las sentencias más relevantes a efectos de determinar cuándo se considera cometido el tipo básico de 278 del Código Penal es la AAP Castellón 2039/2022, de 28 febrero[102] que entiende que para que el delito previsto en el artículo 278 pueda entenderse cometido es necesario que el autor no co-

---

101. SAP Valencia, a 16 de septiembre de 2022. Roj: SAP V 2961/2022 - ECLI:ES:APV:2022:2961. Id Cendoj: 46250370022022100162. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/57e3fe35726c49c3a0a8778d75e36f0d/20221025

102. AAP Castellón, a 28 de febrero de 2022. Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039A. Id Cendoj: 12040370022022200755. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/435fd1c6dfc89317a0a8778d75e36f0d/20231227

nozca el secreto y trate de descubrirlo. Además, establece que se debe tener intención, por lo tanto, de descubrir un secreto de empresa.

> «El delito del artículo 278, 1 del Código Penal es un delito que puede cometer cualquier persona, y no se trata de un delito especial propio que solo está al alcance de quienes reúnen determinadas características, como ocurre con el delito del art. 279, y ha de ser cometido por quien no conoce el secreto, y trata de descubrirlo. En este supuesto el trabajador, lógicamente, conocía los partes de trabajo suyos. Es un delito de consumación anticipada. Basta la acción de apoderamiento dirigida a alcanzar ese descubrimiento. Conseguir el conocimiento del secreto pertenece a la fase posterior de agotamiento de la infracción. Incluso se comete, aunque no pueda después alcanzarse ese descubrimiento del secreto porque, por ejemplo, el autor del delito no puede llegar a descubrir las claves utilizadas por la empresa en defensa de tal secreto. Y su difusión, revelación o cesión a terceros constituye la figura agravada del art. 278. La conducta sancionada en este tipo penal se define a través de tres notas: 1.- El apoderamiento de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran a un secreto empresarial (ya que a éste hay que entender gramaticalmente referida la expresión «al mismo»), o 2.- De modo alternativo, la utilización de alguno de los medios o instrumentos contemplados en el art. 197.1, y 3.- La finalidad de descubrir un secreto de la empresa.»

El Tribunal Supremo ha estudiado los requisitos necesarios para la consumación en la STS 864/2008, 16 de diciembre de 2008[103] al disponer que:

---

103. TRIBUNAL SUPREMO.STS 864/2008, 16 de diciembre de 2008. Roj: STS 7442/2008 - ECLI:ES:TS:2008:7442. Id Cendoj: 28079120012008100954. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/ca4dddcef35a60e6/20090219

> «Es un delito de consumación anticipada. Basta la acción de apoderamiento dirigida a alcanzar ese descubrimiento. Conseguir el conocimiento del secreto pertenece a la fase posterior de agotamiento de la infracción. Incluso se comete, aunque no pueda después alcanzarse ese descubrimiento del secreto porque, por ejemplo, el autor del delito no puede llegar a descubrir las claves utilizadas por la empresa en defensa de tal secreto».

5.5. TIPO SUBJETIVO

El elemento subjetivo se aplica a todas las modalidades de apoderamiento contempladas en el artículo 278.1 del Código Penal que, necesariamente, exige la concurrencia del dolo.

Entendiendo el dolo como la plena conciencia y voluntad de llevar a cabo los elementos objetivos que configuran el delito[104], en el caso específico del espionaje empresarial, regulado en el artículo 278.1 del Código Penal, el dolo debe entenderse como la clara conciencia y voluntad del sujeto activo respecto a varias circunstancias críticas:

1. Conciencia de sustracción: El sujeto activo es plenamente consciente de que está extrayendo información empresarial confidencial, ya sea apropiándose de ella física o intelectualmente, o mediante el uso de tecnologías avanzadas.
2. Reconocimiento de la propiedad ajena: Tiene la plena certeza de que la información que está sustrayendo no le pertenece.
3. Acceso no autorizado: Es consciente de que ha accedido a un ámbito de confidencialidad sin tener autorización, diferenciándose claramente de los casos en los que el sujeto cree erróneamente tener derecho de acceso, lo cual constituiría un error de tipo.

---

104. DÍEZ RIPOLLÉS, J. L.: Derecho Penal Español. Op. Cit., p. 188

El dolo en este delito no incluye la intención de incrementar el número de personas que conocen la información secreta, excepto en lo que respecta al propio sujeto activo que se apodera de ella, tal como señala BAJO FERNÁNDEZ[105]. Esta ampliación en el número de conocedores se asocia más bien con el segundo supuesto del artículo 278 del Código Penal, que se refiere específicamente a la conducta de revelar dicha información.

Dado que es necesaria la concurrencia del dolo, es claro que no cabe punir el hecho si se cometiera por imprudencia, dada la falta de previsión legal, sin perjuicio de que haya autores como MOLINA GIMENO que entienden que sí sería posible (Molina Gimeno, 2009)[106].

A parte de la concurrencia del dolo, en el caso del artículo 278.1 concurre otro elemento subjetivo de lo injusto, que es la finalidad buscada con la realización de la conducta.

El elemento subjetivo de lo injusto desempeña múltiples roles dentro de la estructura del tipo penal, tales como contribuir a la definición precisa del injusto cuando la mera descripción objetiva resulta insuficiente, delimitar claramente este delito de figuras jurídicas similares, facilitando así la resolución de complejidades concursales, y ejercer una función restrictiva[107]. Esta última, como se ha analizado al abordar los límites a la inmaterialidad del apoderamiento, representa una de las contribuciones esenciales del elemento subjetivo de lo injusto en el delito en cuestión, limitando su ámbito de aplicación. Por lo tanto, es imperativo que este elemento ejerza sus funciones de manera efectiva, proporcionando así una herramienta valiosa para la interpretación de los tipos penales y su implementación en el proceso penal.

---

105. BAJO FERNÁNDEZ, M. / BACIGALUPO SAGGESE, S.: Derecho penal económico. Op. Cit., p. 543.

106. MOLINA GIMENO, F. *Conveniencia político criminal de introducir la modalidad imprudente para complementar la protección penal de los secretos de empresa*. Diario La Ley. ISSN 1989-6913, Nº 7123, 2009.

107. DÍEZ RIPOLLÉS, J. L.: *Derecho penal Español*. Op. Cit., p. 185.

No obstante, la interpretación del término «descubrir» no ha alcanzado un consenso dentro de la doctrina y la jurisprudencia, generando un debate que otorga a este elemento un carácter disruptivo. Hasta el momento, la jurisprudencia ha adoptado principalmente dos interpretaciones: por una parte, se entiende el elemento subjetivo «para descubrir un secreto de empresa» como el «ánimo de conocer»; por otra, se interpreta como el «ánimo de revelar» dicho secreto. A estas dos interpretaciones, ampliamente respaldadas tanto por la jurisprudencia como por la doctrina, un sector doctrinal añade una tercera perspectiva, que incluye el «ánimo de revelar y utilizar» la información descubierta.

Todo ello ha llevado a la jurisprudencia a entender que estamos ante un delito de intención trascendente, porque la finalidad perseguida por el autor está intrínsecamente unida a la realización de la conducta. Y además también la jurisprudencia ha entendido que es un delito mutilado de dos actos, dado que existe una materialización externa de la finalidad en un acto que el autor realiza con la intención de descubrir el secreto, independientemente de que obtenga el resultado deseado o no.

Al respecto hemos de hacer referencia a dos sentencias importantes. Por un lado, en cuanto a la necesidad de la concurrencia de la finalidad, la AAP Castellón 118/2022, de 28 de febrero de 2022[108].

> «Como hemos indicado la acción típica, es el apoderamiento de los datos, y la misma ha de estar encaminado a una finalidad típica, como es la de « descubrir un secreto de empresa», finalidad que se erige en un elemento subjetivo del injusto que ha de quedar igualmente probado. Esta finalidad típica parece sugerir que lo que se está sancionando es exclusivamente el llamado espionaje industrial. El hecho de que este precepto penal esté incluido en la Sección

108. AAP Castellón 118/2022, de 28 de febrero de 2022. Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039A. Id Cendoj: 12040370022022200755. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/435fd1c6dfc89317a0a8778d75e36f0d/20231227

dedicada a los «delitos relativos al mercado y a los consumidores» indica que el bien jurídico protegido es de modo primario la defensa de la libre competencia y con ello la defensa de la empresa frente a intromisiones ilícitas de otros competidores que puedan perjudicar su posición en el mercado a través del conocimiento de datos reservados de la propia empresa.»

«La finalidad típica se limita a la intención de descubrir el secreto, sin que se exija ninguna motivación especial, como podría ser la de perjudicar al empresario. De este modo lo que ha de quedar acreditado es la voluntariedad de que la acción de apoderamiento de los datos tiene precisamente como finalidad la de entrar en conocimiento de ello, sin que el motivo de esta actuación o la finalidad de segundo grado que se pretenda tras el descubrimiento se configure ya como requisito del tipo».

En lo que respecta a la consideración de esa intención como parte inescindible de la conducta típica la STS 1607/2000, de 16 de febrero, que afirma que «no en balde, la norma emplea la preposición «para» en el sentido de «tener intención» de revelar secretos, de tal manera que si no se prueba esa intencionalidad la acción deviene atípica». Esta posición está apoyada por gran parte de la doctrina, entre los que hemos de destacar a PRATS CANUTS que realizando una visión finalista del artículo 278.1 al albor de las palabras para descubrir un secreto de empresa, otorga al presente precepto la caracterización de un «delito de tendencia interna intensificada, en donde la acción debe de estar presidida por la voluntad de descubrimiento, lo cual exige que el ánimo sea previo o coetáneo a la realización del comportamiento típico. Ello obliga a concluir que el apoderamiento desprovisto de la voluntad de descubrimiento es atípico. Por tanto, los descubrimientos fortuitos no son subsumibles en el tipo penal, desplegando así dicho elemento subjetivo del injusto la función selectiva y restrictiva a la cual hacíamos antes mención» (Prats Canut, 1997)[109].

---

109. Prats Canut, J. *Descubrimiento y* ...op, cit., p. 16.

La jurisprudencia también ha entendido que la finalidad de descubrir debe ser identificada o equiparada al ánimo de revelar el secreto. Las dudas se podrían plantear sobre si al utilizar el legislador la palabra descubrir, está incluyendo en este verbo únicamente los actos que implican conocer, o pueden entenderse incluidos también las conductas de revelar. Acojamos una u otra postura lo cierto es que, la realización de la conducta descrita en el artículo 278, que implican en todo caso un acceso indebido a la información, lleva implícita que el autor se coloca en una situación de dominio sobre el secreto, que le favorece tener mayores facilidades para la revelación del mismo en un futuro. Esto no implica que la conducta del autor vaya siempre dirigida a la revelación a posteriori de los secretos indebidamente conocidos, porque ello supondría dejar impune los actos de descubrimiento si se buscara sólo la explotación del secreto por parte del autor, esto es, como considera MÁRTINEZ BUJÁN PÉREZ, podrían quedar impunes «los casos en que el autor lleve a cabo el apoderamiento del secreto con ánimo de utilizarlo el mismo». Por eso este autor entiende que «la finalidad de descubrir debería entenderse integrada por el ánimo de revelar y utilizar el secreto»[110]. Y ello porque entiende que realmente se está afectando a los intereses del empresario con igual gravedad se realice un acceso indebido, o se revele la información obtenida. A pesar de estas valoraciones doctrinales, lo cierto es que, con el delito de descubrimiento de secretos de empresa, lo que intenta evitar el legislador penal son los perjuicios que indudablemente las empresas sufren cuando personas no autorizadas para acceder a información secreta, no sólo acceden, sino que la revelan y utilizan en perjuicio de la empresa afectada. Se intentan evitar situaciones en las que se aproveche ilícitamente de los beneficios derivados de la posesión del secreto. Esta es la razón última de la tipificación de las conductas. Por eso bastaría el acceso indebido y el apoderamiento para entender la conducta cometida, sin que sea necesario un acto de utilización

110. MARTÍNEZ-BUJÁN PÉREZ, C. *Delitos relativos*…op, cit,. p.41.

o explotación posterior por parte del autor de los hechos. A su vez, otra razón para defender esta postura es el hecho de que, si efectivamente se realizan actos dispositivos sobre el secreto indebidamente obtenido, las conductas quedarían fuera de la tipificación del artículo 278.1 y serían castigadas por la vía del artículo 278.2.

Por otro lado, en el caso de que el autor de los hechos proceda a acceder y apoderarse del secreto de empresa sin estar legitimado para ello, pero lo mantiene en su poder, en previsión de poder utilizarlo en un futuro a su favor, sin que haya realizado actos de revelación, explotación o uso del secreto, la conducta entraría dentro de las previstas en el artículo 278.1.

En función de todo lo que hemos dicho anteriormente, la postura inicial más adecuada sería entender que la finalidad de descubrir es elegida por el precepto penal implica que concurre en el autor de los hechos un ánimo de conocer el secreto. Y es la postura que mantiene la mayor parte de la doctrina, y que podemos ver en alguna sentencia como por ejemplo SAP Sevilla 593/2007, de 19 de octubre en la cual se entiende lo siguiente:

> «La finalidad típica cifrada en descubrir un secreto de empresa debe identificarse con la finalidad de entrar en conocimiento de ello. Lo que ha de quedar acreditado es la voluntariedad de que la acción de apoderamiento de los datos tiene precisamente como finalidad la de entrar en conocimiento de ello, sin que el motivo de esta actuación o la finalidad de segundo grado que se pretenda tras el descubrimiento se configure ya como requisito del tipo».

Pero a veces también puede suceder el caso de que el autor accede a la información, y la revela o transmite sin haber tenido un conocimiento previo de su contenido. Por ejemplo, si se trata de una información demasiado técnica a cuya comprensión el autor de las conductas delictivas no tiene acceso, o se encuentra transcrita en un idioma que él desconoce. Resulta claro que el autor realiza la conducta de acceso y apoderamiento, pero no conoce el contenido de la información. Y a pesar de que no conozca su contenido, el hecho de que la información

haya quedado bajo su dominio y poder, le posibilita realizar las conductas de revelación o difusión, y obtener en consecuencia el consiguiente beneficio de su explotación económica. Por eso no podríamos entender que el ordenamiento requiere un conocimiento para posibilitar la difusión, puesto que este conocimiento no es indispensable para entender la conducta realizada. Podría por tanto llegar a la conclusión de que la finalidad de descubrir no puede ser considerada como sinónimo de ánimo de conocer por parte del autor de los hechos, sino como «ánimo de poner en conocimiento de otro». BAJO FERNÁNDEZ así lo entiende cuando dice que «obra con ánimo de descubrir aquel que persigue introducir en el ámbito de conocimiento del secreto a alguna persona, lo que se consigue tanto si es el autor quien trata de conocer el secreto como si entrega el objeto a un tercero sin abrirlo», y por tanto sin haber tenido conocimiento de su contenido[111].

En definitiva, para la consumación del delito no es necesario que se haya alcanzado un conocimiento del secreto indebidamente obtenido. Basta que haya quedado en poder del autor de los hechos y que le favorezca una revelación o explotación posterior de la información.

Es especialmente difícil demostrar la concurrencia del dolo en los delitos de revelación y descubrimiento de secretos empresariales, porque en muchas ocasiones ni la empresa es consciente de cómo han sido ejecutados los hechos o qué sistema o medida de protección ha fallado para permitir la comisión de los delitos. A veces los *softwares* utilizados para el apoderamiento del secreto no dejan huella digital alguna, lo que hace difícil demostrar la concurrencia del delito y el ánimo del autor en el conocimiento y descubrimiento de la información. Por eso ha de acudirse a elementos indiciarios en base a los cuales pueda probarse la comisión del delito y la finalidad del descubrimiento de secreto de empresa que el precepto requiere. Estudiar cuáles son los comportamientos del autor de los hechos

111. BAJO FERNÁNDEZ, M. Derecho penal…op, cit., p.19.

antes de proceder al apoderamiento, la variación en sus ingresos, que podrían demostrar el haber explotado económicamente el secreto obtenido, la concurrencia de algún interés profesional del autor de los hechos, que por tener la consideración de competidor con la empresa cuyo secreto ha sido revelado, podrían ser tomados en consideración para entender que el autor sí tiene un interés en perjudicar los derechos de competencia de la empresa afectada.

La conducta de apoderamiento implica la utilización de medios ilícitos para el acceso al secreto. En el caso de que se procediera al robo o hurto de los soportes informáticos en los que éste se encuentra, no cabría duda de la necesidad de aplicar la figura del concurso de delitos. En las ocasiones en las que se hayan violado las medidas de seguridad para poder acceder indebidamente a un sistema informático, el concurso podría darse con el delito de sabotaje informático del artículo 264 bis.

Continuando con el análisis de los elementos subjetivos del tipo, la concurrencia de la voluntad o ánimo de descubrir secretos por parte del autor como un elemento que indispensablemente ha de concurrir en la conducta para entender cometido el delito es claramente coherente con lo estipulado en la «Ley de Competencia Desleal». De hecho, en el artículo 13.3 de esta Ley se dispone claramente que «será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio de un tercero, o de perjudicar al titular del secreto».-

La demostración del dolo en el delito de usurpación de secretos empresariales, contemplado en el artículo 278.1 del Código Penal, junto con la prueba del elemento subjetivo del tipo penal, representa un desafío particularmente complejo. Un análisis detallado de la jurisprudencia revela una abundancia de casos en los que se dicta sentencia absolutoria debido a la insuficiencia de pruebas incriminatorias[112].

---

112. En este sentido, entre otras, la SAP Barcelona (Sección 7ª), 104/2000, de 11 de febrero, el AAP Madrid (Sección 7ª) 215/2002, de 7 de mayo, la SAP Valencia 154/2002, de 17 de junio, la SAP Valencia (Sección 5ª), 151/2002, de

Dado que la obligación de probar recae sobre la acusación, es frecuente encontrar en estos fallos que la empresa denunciante no logra demostrar de manera convincente lo alegado en su denuncia, fallando en proporcionar información detallada o en presentar datos específicos. No obstante, es crucial reconocer que la dificultad para probar la apropiación indebida de secretos empresariales radica en la naturaleza intangible del bien sustraído. Esto conlleva a que, en muchas ocasiones, tal conducta apenas deje huellas, ya que no necesariamente implica la desposesión física del titular. Esta particularidad obstaculiza significativamente que la parte acusadora pueda presentar pruebas directas de la comisión del ilícito.

La presencia de elementos subjetivos en la definición del delito debería facilitar la resolución de los casos ante los tribunales, en lugar de complicar el proceso judicial o conducir prematuramente a absoluciones y sobreseimientos por la imposibilidad de probar dichos elementos. Sin embargo, la complejidad en la demostración de estos componentes esenciales ha sido destacada por la doctrina, debido a que reflejan una intención o predisposición subjetiva, la cual puede inferirse, pero no observarse directamente. Por lo tanto, resulta imprescindible identificar ciertos indicadores objetivos que permitan inferir la intención de actuar en detrimento de un bien jurídico protegido.

Estos indicadores objetivos constituyen la base de la prueba indiciaria, partiendo del principio de que si los indicios son válidos, también lo es el hecho que determina la culpabilidad del acusado. Este tipo de prueba es fundamental en la resolución de numerosos delitos y resulta especialmente relevante en este contexto, como lo demuestra la resolución AAP Madrid (Sección 30ª), 439/2011, de 18 de julio, que subraya la necesidad de

---

19 de junio, el AAP Castellón (Sección 1ª), 270/2006, de 15 de mayo, la SAP Barcelona (Sección 8ª), 178/2011, de 28 de febrero, la SAP Vizcaya (Sección 6ª), 821/2011, de 4 de noviembre o la SAP Ciudad Real (Sección 1ª), 19/2012, de 17 de septiembre.

recurrir a la prueba indiciaria, cuya evaluación conjunta debe realizarse tras la vista oral.

Existen casos en los que claramente no hubo intención de apropiarse de información empresarial, como el AAP Islas Baleares (Sección 2ª), 113/2005, de 8 de junio, que rechazó el recurso contra la absolución previa, al considerar que el desvío de un número de fax fue un error involuntario, sin intención de apoderarse de secretos empresariales. En contraste, hay situaciones en las que la existencia del dolo es evidente, como en la SAP Asturias (Sección 2ª), 523/2014, de 18 de noviembre, donde la condena se basó en una sólida actividad probatoria. Asimismo, el AAP Guipúzcoa (Sección 3ª), de 30 de septiembre de 2004, sugiere que las diligencias iniciales deben incluir la inspección de la empresa acusada y una pericial judicial complementaria para verificar la apropiación de secretos empresariales.

No obstante, la obtención de pruebas claras no siempre es posible, especialmente en lo referente a los elementos subjetivos del delito. Aquí, la prueba indiciaria adquiere una importancia crucial. Para que esta sea considerada suficiente para la incriminación, es necesario que los indicios sean múltiples y variados, ya que un único indicio raramente fundamenta una condena penal, salvo en circunstancias excepcionales de singular relevancia.

Entre los posibles indicios que pueden evidenciar la comisión de este delito se incluyen: comportamientos previos al apoderamiento, contradicciones en las declaraciones del acusado, la relación del sujeto con empresas del mismo sector y posibles vínculos con la información sustraída, como el traslado de una cartera de clientes o la aparición en el mercado de productos que incorporen información o fórmulas protegidas.

En conclusión, estos y otros hechos circunstanciales pueden ofrecer una prueba suficiente de la existencia del dolo y del elemento subjetivo del tipo penal en el delito de apropiación de secretos empresariales, siendo esencial analizar cada caso en detalle para identificar los elementos probatorios pertinentes.

5.6. EL CIBERESPIONAJE

El espionaje puede efectuarse a través de un acceso remoto o telemático, es decir, en un entorno virtual sin necesidad de interactuar físicamente con el equipo objetivo.

Esta modalidad de espionaje se caracteriza por la interceptación de telecomunicaciones, empleando dispositivos técnicos especializados en la escucha, transmisión, grabación o reproducción de sonidos, imágenes o cualquier otro tipo de señal comunicativa. Este enfoque se fundamenta en la legislación referente a las denominadas «escuchas ilegales», incorporadas al Código Penal anterior mediante la LO 7/1984, de 15 de octubre, y posteriormente ampliadas por la LO 18/1994, de 23 de diciembre, para incluir la captura de imágenes y la interceptación general de comunicaciones[113].

Con la inclusión de estas prácticas, se buscaba prevenir la captación ilícita de comunicaciones confidenciales dentro del ámbito empresarial, tanto en entornos de telecomunicaciones como en interacciones presenciales, siempre mediante el uso de medios técnicos. Aunque inicialmente esta conducta se legisló en un contexto donde la comunicación telefónica era predominante, el auge de internet desde principios de los años 90 como medio de comunicación a distancia exige una interpretación actualizada que abarque las nuevas formas de comunicación digital y el uso de tecnologías de la información y la comunicación (TICs).

En cuanto al objeto de la interceptación, este recae sobre las telecomunicaciones, definidas en la actualidad como el sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos[114]. Esta definición su-

---

113. ANARTE BORRALLO, E. Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información, en Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, nº1, 2001, p. 55.

114. Única acepción del término del Diccionario de la Real Academia de la Lengua Española. Recurso electrónico disponible en: http://lema.rae.es/drae/?val=telecomunicaci%C3%B3n

braya que la acción de interceptar se desarrolla íntegramente en un espacio virtual, excluyendo las interacciones directas en un mismo lugar físico.

En la era digital actual, las formas de comunicación telemática más predominantes son el teléfono y las redes informáticas, tanto internas (como las intranets) como externas (como Internet).

Entre los métodos de ataque a estas tecnologías, es importante resaltar el «pinchazo» telefónico. Sin embargo, en el ámbito de las redes informáticas, la diversidad de técnicas de ataque se ha expandido de manera exponencial, convirtiéndose en el principal escenario para el ciberespionaje. Este último se caracteriza por emplear métodos altamente sofisticados para el almacenamiento y acceso ilegítimo de información, constituyendo la forma más prevalente de espionaje digital.

Hoy en día, la presencia online es un requisito indispensable para cualquier empresa, con la mayoría de sus datos almacenados digitalmente. Esto incrementa significativamente los riesgos de sufrir ataques cibernéticos. Tendencias actuales como la migración de datos a la nube y el uso extendido de dispositivos móviles para acceder a redes corporativas internas complican aún más la protección de la propiedad intelectual de las organizaciones[115]. Este desafío se intensifica en el caso de las pequeñas y medianas empresas, que suelen concentrarse en actividades específicas y, a menudo, no cuentan con programas de ciberseguridad efectivos. Es crucial reconocer que la gran mayoría de las empresas en nuestro país se enfrentan a esta realidad[116].

---

115. BRADLEY, T. McAfee: Corporate Espionage is the Currency of Cybercrime, PcWorld, 28 de marzo
de 2011. Recurso electrónico disponible en: https://www.pcworld.com/article/223483/mcafee_corporate_espionage_is_the_currency_of_cybercrime.h

116. De acuerdo con la información proporcionada por el Directorio Central de Empresas (DIRCE) y publicada por el Ministerio de Industria, Energía y Turismo en febrero de 2016, la inmensa mayoría del tejido empresarial en España, representando un 99,88% que se traduce en 3.178.408 entidades, está

Dentro de las técnicas más destacadas de ciberespionaje se encuentran los programas rastreadores o «sniffers», que capturan datos que transitan por la red mediante un software ejecutado en un dispositivo conectado a ella o a través de un aparato vinculado directamente al sistema de cableado. Otro método relevante es la minería de datos o «data mining», una tecnología que permite descubrir información valiosa y previamente desconocida, analizando grandes volúmenes de datos con técnicas estadísticas avanzadas. Además, el uso de programas maliciosos (malware) por parte de piratas informáticos o «hackers» facilita el acceso no autorizado a información sensible en el ciberespacio, lo cual podría considerarse una forma de interceptación de las telecomunicaciones cuando se realiza de manera remota. Sin embargo, es fundamental entender que estas acciones no se limitan a un simple acceso ilícito a la información, ya que esto constituiría un delito de intrusismo informático, tal como se establece en el artículo 197 bis del Código Penal. Es imprescindible que de dicho acceso se derive la obtención de información que se clasifique como secreto empresarial para que se considere ciberespionaje.

Así, por ejemplo, las páginas web de instituciones clave en Estonia, incluyendo el Congreso, la Presidencia y el Primer Ministro, fueron objeto de ataques y bloqueos durante varios días. Estos incidentes se produjeron simultáneamente con la controvertida decisión del Gobierno estonio de reubicar una estatua emblemática de la Segunda Guerra Mundial, conocida como el Soldado de Bronce de Tallín. Este monumento era venerado por la comunidad rusa como un homenaje a sus caídos en el conflicto, siendo tradición depositar flores a sus pies en fechas conmemorativas. Sin embargo, para muchos estonios, el soldado representa un doloroso recordatorio de la opresión soviética.

La reacción no se hizo esperar. El Gobierno ruso y las minorías étnicas rusas en Estonia expresaron su firme protesta. En

---

compuesta por pequeñas y medianas empresas (PYME). Recurso electrónico disponible en: https://ipyme.org/es-es/Paginas/default.aspx

foros rusos, se alentó la participación en ataques cibernéticos contra Estonia, empleando tácticas como «botnets» y «defacements» para inundar y alterar sitios web estonios con propaganda, afectando no solo a las instituciones inicialmente mencionadas, sino también a servicios esenciales como la policía, y los ministerios de Economía, Agricultura, Medio Ambiente, Asuntos Exteriores y el Departamento de Comunicaciones.

La magnitud del caos cibernético obligó a una respuesta internacional coordinada por varios CERTs y a la desconexión temporal de Estonia de la red global, para salvaguardar sus servicios internos en línea. Este incidente no solo marcó un precedente para Estonia sino que también resonó a nivel mundial, con países como EE.UU., Reino Unido, Francia, y Alemania reportando ataques similares. Este evento significó un desafío sin precedentes para la OTAN, que por primera vez vio a uno de sus miembros solicitar apoyo frente a una amenaza cibernética, llevando a la adopción de una política de ciberdefensa en enero de 2008 y a la creación del Centro de Excelencia para la Cooperación en Ciberdefensa en Tallín.

Este centro, con la participación de países miembros como España, Italia, Alemania, Eslovaquia, Estonia, Letonia, EE.UU., Hungría, Lituania y Turquía, se erige como un bastión contra las amenazas cibernéticas. Su misión, delineada en su memorándum fundacional, abarca la protección contra ciberataques, la formación de personal militar, la investigación en defensa electrónica, el desarrollo de un marco legal adecuado, y la implementación de soluciones globales a desafíos específicos. Para ello, cuenta con equipos multidisciplinarios de expertos en ciberseguridad, especializados en áreas operativas, tecnológicas y legales. El centro opera bajo la dirección de un comité compuesto por representantes de los países miembros y de la OTAN, consolidándose como una Organización Militar Internacional dedicada a la vanguardia de la ciberdefensa[117].

---

117. SÁNCHEZ MEDERO, G. *El ciberespionaje.* Revista Derecho.com ISSN: 1988-2629. No. 13. Nueva Época. Marzo-Mayo, 2013.

6. El Artículo 278.2. El tipo cualificado: la revelación de secretos de empresa

La conducta de revelación de secretos de empresas se encuentra tipificada en el artículo 278.2 y reza «Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos». Si esta conducta es realizada por quien tiene obligación de guardar reserva, resultaría castigada por la vía del artículo 279.1. Y si las conductas de revelación son cometidas por el que conoce el origen ilícito, pero no tomando parte en los actos físicos de descubrimiento, la conducta sería subsumible en el tipo del precepto 280.

Como vemos es necesario realizar un análisis de los elementos que rodean la revelación de secretos de empresa, porque la concurrencia de uno u otro determinará la aplicabilidad de uno u otro precepto. Existen varias modalidades para la comisión del delito: con infracción del deber de reserva, sin haber tomado parte en el descubrimiento, o realizando la conducta simplemente de manera ilícita. Todas tienen en común que el autor de los hechos accede ilícitamente a la información empresarial con intención de hacer entrega de la misma a terceros, y obtener como consecuencia de tal conducta rendimiento o beneficios propios o ajenos. Pero la variedad de acciones ha motivado que existan resoluciones jurisprudenciales que llegan a confundir los casos en los que resultan aplicables uno u otros preceptos penales, tipificando como conductas del artículo 280 las deberían ser subsumidas en el artículo 278.1, o no castigando las

conductas por la vía del artículo 279 porque el autor de los hechos no tenía deber de reserva sobre los secretos descubiertos.

Respecto al sujeto activo del delito la AAP Castellón, a 28 de febrero de 2022 aclara que «El delito del art. 278, como se ha visto ha declarado el Tribunal Supremo, no es un delito especial pero sí exige que quien accede al secreto no lo conozca ya, lo que le diferencia del art. 279, este sí es un delito especial».

6.1. ELEMENTOS OBJETIVOS DEL SUPUESTO AGRAVADO

A tenor literal de lo dispuesto en el artículo 278.2, las conductas de difusión, revelación o cesión a terceros de los secretos descubiertos han de ser realizadas por aquel que previamente se hubiera apoderado de los mismos, esto es, es necesario que haya cometido previamente las conductas descritas en el artículo 278.1 Por lo tanto el mismo sujeto activo que comete las conductas descritas en el artículo 278.1 es el mismo que comete las definidas en el apartado 2 que contempla el supuesto agravado.

En el supuesto agravado no se le exige al autor de la revelación que concurra un ánimo de conocer o descubrir el secreto. No se le exige que haya existido un conocimiento de su contenido, para poder entender que la conducta se realiza. Lo que siempre es relevante es que haya una consciencia por parte del autor de los hechos de que la revelación, difusión o cesión se está realizando sobre secretos de empresa, siendo consciente de la utilidad de ésta y de que su posesión o dominio puede generar perjuicios en la persona del propietario de la empresa cuyo secreto ha sido revelado pues puede favorecer ilícitamente a competidores o terceros interesados en conocer el secreto.

Las conductas de difusión, revelación y cesión contempladas en el supuesto agravado son castigadas con la misma pena, porque el legislador penal entiende que estas conductas implican el mismo desvalor de acción. Entre ellas existen pequeños matices, pero las conductas son homologables y a efectos penales reci-

ben el mismo tratamiento, porque la afectación del bien jurídico es el mismo y el desvalor de la conducta es equiparable.

6.2. DEFINICIÓN DE LAS CONDUCTAS CASTIGADAS: DIFUSIÓN REVELACIÓN Y CESIÓN

La Real Academia Española considera que difundir es «propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc». Difundir implica la voluntad de que el conocimiento se extienda a terceros. Supone por lo tanto que el secreto es transmitido más allá del grupo de personas que originariamente conocían el secreto, y esa transmisión conlleva cierta amplitud, posibilitándose con las conductas que un número considerable de terceras personas puedan tener conocimiento del secreto, cuando éste había sido debidamente protegido para que sólo pudiera ser conocido por un número muy limitado de personas. La difusión implica extender el conocimiento, y no se requiere un número concreto de destinatarios de la difusión o revelación, pudiendo tratarse de un número indeterminado de personas, o incluso de un número que pueda ser ampliable en un futuro. Puede ser que el autor de la revelación revele el secreto a un grupo de personas, pero debe ser plenamente consciente de que al exteriorizar el contenido del secreto y ponerlo en poder de terceros, éstos tendrán la posibilidad de transmitirlo a su vez a otro grupo de personas, con lo que las posibilidades de extensión del conocimiento podrían ser ilimitadas.

En cuanto al verbo «revelar», la Real Academia Española lo define como «descubrir o manifestar lo ignorado o secreto». CARRASCO ANDRINO entiende, que tanto la revelación como la difusión «implican la transmisión del secreto a terceros, sin que baste con la simple captación del secreto por el sujeto activo»[118].

---

118. CARRASCO ANDRINO, M. *La protección penal del secreto de empresa*. Madrid.1998. Págs

Aunque no se exige expresamente, resulta claro que la revelación tendrá un número considerable de destinatarios, a veces no siendo realmente conocida por el autor las posibilidades de expansión de su conducta de revelación, cuestión que ya hemos analizado hace unos momentos en cuanto a la conducta de difusión de difundir.

Hay parte de doctrina que entiende que no es necesario diferenciar entre el término difundir o revelar, porque lo entienden sinónimos o equivalentes. Pero de hecho también desde el punto de vista normativo, nuestro ordenamiento en muchas ocasiones ha procedido a identificar estas dos conductas, llegando incluso a confundirlas. Si analizamos lo dispuesto en el artículo 13 de la «Ley de Competencia Desleal», no observamos que se diferencie entre las conductas de difusión y revelación. De hecho, se usa el término divulgar, y en él se abarcan todas las conductas que implican la comunicación del secreto a un tercero diferente al autor. Y ello con independencia del número de destinatarios del acto de revelación o de las personas que finalmente conozcan el contenido del secreto.

A nivel europeo la «Directiva UE 2016/943 prefiere la utilización del término revelar. Por ello analizando el contenido de nuestras normas, y el tratamiento que la jurisprudencia realiza de las conductas, podemos considerar prácticamente sinónimos los términos de difusión o revelación. Ambos implican la transmisión del conocimiento del secreto a terceros ajenos al mismo y por tanto una ampliación del número de personas que acceden indebidamente a la información. No obstante, sí existe parte de doctrina que entiende que en la difusión hay un mayor desvalor que en la revelación. CARRASCO ANDRINO entiende que «difundir consistirá en comunicar a un número indeterminado de sujetos, lo que produce la eliminación del bien económico, que se apoya en el mantenimiento de la propia situación de secreto, mientras que la revelación, por el contrario, no tendrá un alcance tan general ni supondrá, en principio, la destrucción del secreto en cuanto tal, aunque sí la afectación, al menos como idoneidad para lesionar, del interés económico en el mantenimiento del secreto». Como vemos la autora realiza una deli-

mitación precisa de la difusión, y la concibe con mayor gravedad que los actos de revelación.

El Código Penal parece ofrecer una definición de revelación al tratar los «delitos de descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional». Concretamente el artículo 599.2 del Código Penal impone una agravación en los casos en los «que la revelación consistiera en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión». Por otro lado, también en los «delitos relativos a la intimidad», contemplados en los artículos 197 y siguientes del Código Penal, resulta claro que cuanto mayor sea el número de personas conocedoras del secreto o información que afecta a la esfera íntima de un individuo, mayor será la afectación de los derechos de intimidad y mayor el desvalor de la acción. Y si el legislador no ha contemplado una agravación en función del número de personas a las que se difunde o revela el secreto en una materia tan sensible como las informaciones que afecten a la esfera privada y a la intimidad de los ciudadanos, tampoco resultaría lógico entender que el legislador penal en los delitos de revelación de secretos de empresa, haya pretendido requerir una extensión concreta en el número de personas conocedores de la información tras la revelación. Además el bien jurídico protegido en los delitos de descubrimiento y revelación de empresas, que es el interés del empresario en la salvaguardia del secreto para la protección de sus capacidades competitivas y beneficios económicos, es mucho menos relevante que la afectación de derechos tan fundamentales como la intimidad de las personas. La revelación de datos personales e íntimos causa mayor impacto personal y psicológico, y los daños morales derivados de su revelación son mucho mayores que los datos ocasionados a la empresa que sea víctima de un delito de revelación de sus secretos, aun cuando sean cuantificables económicamente.

La tercera conducta que hemos de analizar es la cesión. El Diccionario de la Real Academia Española define cesión como «dar, transferir, tras pasar a alguien una cosa, acción o derecho». A pesar de ser éste el sentido gramatical, lo que resulta

claro es que la conducta de cesión tipificada en el supuesto agravado del artículo 279.2 supone que se le comunica el secreto a una o varias personas no autorizadas para tener tal conocimiento. La agravación radica en el hecho de la comunicación, esto es, en la conducta que implica el traspaso del conocimiento a terceros no autorizados.

Un supuesto bastante frecuente de cesión se produce en aquellas ocasiones en las que el trabajador infringiendo el deber de reserva que le vincula con la empresa, conoce datos e informaciones o secretos por la prestación de sus servicios laborales en la misma y procede a reenviarse a sí mismo esos datos vía email, o por otros mecanismos de transmisión a cuentas de almacenamiento personales, o procede simplemente almacenar a los datos, sin cederlos a terceros. Este es un supuesto conocido como auto cesión que estudia la STS 285/2008, de 12 de mayo[119] en la cual se dispone que

> «De cualquier modo hay que tener presente que ambos acusados se incurrieron en la conducta típica de cesión (dentro de la que hay que sin duda incluir la auto cesión) de los secretos de empresa, contraviniendo la obligación legal que, como fuente de la reserva, les venía imposta por su condición de empleados de la empresa y por su contrato laboral, habiendo accedido a tal información durante la vigencia del contrato y antes de extinguirse la relación laboral»

El ordenamiento jurídico contempla también un concepto de cesión en la normativa relativa a la protección de datos personales, la cual enraíza directamente con los delitos relativos a la intimidad de los artículos 197 y siguientes del Código Penal, los cuales a su vez suelen ser utilizados como base para el estudio de los elementos del tipo de los delitos de revelación de se-

---

119. TRIBUNAL SUPREMO. STS 285/2008 de 12 de mayo de 2008. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703

cretos empresariales. Por ello quizás sería adecuado tener en consideración la definición que de cesión realiza la «Ley Orgánica 15/1999, de 13 de protección de datos de carácter personal» en el artículo 3. Concretamente en el apartado i) se define la «cesión o comunicación de datos» como «toda revelación de datos realizada a una persona distinta del interesado». Somos conscientes de que el «Real Decreto 1720/2007 de 21 de diciembre», que aprueba el Reglamento de desarrollo de la «Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal», excluye de su ámbito de aplicación todo lo relativo a los secretos empresariales. Así en su artículo 2 dispone que

> «2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
>
> 3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.»

Pero ello no es obstáculo para poder remitirnos a esta normativa a la hora de poder conceptualizar cuál debe ser el contenido del término «cesión» utilizado por el legislador penal al tipificar las conductas de revelación de secretos empresariales.

Lo que sí resulta claro es que la difusión de por sí parece contener una cierta extensión. Cuando los datos o los secretos se difunden, llegan a conocimiento de un gran número de personas, no quedando éste limitado a un círculo reducido, sino conllevando una conducta de generalización del conocimiento, que quizás supone un mayor desvalor de acción y una mayor afectación de los derechos del empresario que pretenden ser salvaguardados mediante la tipificación penal. Algunos autores han entendido que la difusión es «la revelación o cesión realiza-

da a un gran número de destinatarios». Esta postura es defendida entre otros por CARRASCO ANDRINO, que también ha realizado una diferenciación entre cesión y revelación. Así ha afirmado que «interpretando la cesión como transmisión de algo por medios informáticos, obliga a inferir que la única posibilidad de diferenciarla de la revelación sería entender que, mientras que esta última supone el conocimiento por el receptor de haber recibido un secreto por serle entregado el soporte material del mismo, la primera (recordemos, la cesión) conllevaría el desconocimiento de la recepción por el destinatario del secreto»[120]. Esta autora también entiende que el término cesión implica cierta intención de legislador de considerar la transmisión del soporte material en la que el secreto se contiene, pero no podemos obviar, en una sociedad tecnológica, que la cesión a veces se realiza por medios telemáticos, y no requieren el desplazamiento físico de los soportes que contienen los secretos e informaciones (Carrasco Andrino, 1998).

Sea las conductas de difusión, revelación o cesión, todas ellas tienen en común que mediante su realización se posibilita que terceros no autorizados conozcan el contenido de informaciones reservadas, y por el hecho de haber accedido a tal conocimiento, se las coloca en una situación de dominio y control sobre la información, posibilitándose que puedan explotarla o divulgarla obteniendo considerables beneficios, económicamente cuantitativos, o susceptibles de verse reflejados en un incremento de la competitividad empresarial por parte de los competidores de la empresa cuyo secreto ha sido revelado.

Además sea cual sea la conducta realizada, de las definidas en el supuesto agravado del artículo 278.2 del Código Penal, el secreto deja de tener carácter exclusivo, y se pierde el poder de dominio o de control de la información por parte del empresario titular del secreto. La información llega a conocimiento de terceros a consecuencia de las conductas de difusión revelación

120. CARRASCO ANDRINO, M. *La protección penal*…op., cit., p. 60.

o cesión, y se lesiona los derechos de reserva sobre el secreto por parte del empresario.

A pesar de lo anterior, es indiferente si el conocimiento ha sido alcanzado por uno o varios sujetos, esto es, es irrelevante si se ha revelado el secreto de forma notoria, posibilitando que una multiplicidad de personas no autorizadas accedan a conocer el contenido de la información o si sólo la conducta de difusión, revelación o cesión ha sido realizada en beneficio de una única persona, siendo ésta el único destinatario de la revelación o difusión. Estas conductas son castigadas en todo caso como supuesto agravado del artículo 279.2 sin ninguna excepción.

La STS 285/2008, de 12 de mayo de 2008[121] aclara que,

> «Con ello, dada la naturaleza vulnerable de la información y el valor relativo para la empresa que la posee, derivado de su carácter reservado, su mera comunicación a un sujeto concreto, aun cuando no la convierta en notoria, produce una pérdida potencial de su valor. Por tanto, no es preciso que la información se convierta en notoria para que se dé el efecto material que pretende evitarse con el presente delito y que radica en una pérdida del valor de la información a que da lugar su carácter secreto, bastando sólo con la comunicación a una única persona para que ello se produzca.»

Es acuerdo común de la doctrina entender que es indiferente el tipo de medio utilizado para la comisión del delito. La revelación del secreto puede realizarse por cualquier medio que sea apto para la conducta. Es admisible la forma escrita, oral, la utilización de medios personales de comunicación como correos electrónicos, o la revelación por mecanismos de divulgación masiva como Internet. Todos los medios que sean aptos para la comunicación de información serían admisibles, siem-

---

121. TRIBUNAL SUPREMO. STS 2885/2008 de 12 de mayo de 2008. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703

pre y cuando tengan la capacidad de constituir un peligro para la exclusividad del secreto que ha de ser protegida, y posibiliten al autor la revelación de la información a terceros no autorizados, que pueden aprovecharse del conocimiento del secreto o incluso volver a revelarlo a otros para un más general conocimiento.

Del tenor literal del precepto que regula el supuesto agravado contemplado en el artículo 278.2 resulta claro que estamos ante un delito de resultado que requiere que se haya ocasionado una revelación efectiva de los secretos de empresa, de tal manera que el tercero que adquiere conocimiento del secreto asume una situación de dominio o poder sobre el mismo, que le legitima a disponer de él y a explotarlo, en su propio beneficio o en el de un tercero. Por eso se entiende que para la revelación no es suficiente con la comunicación del secreto, sino que es necesario poner al receptor de la revelación en una situación que le posibilite disponer de la información reservada. Es indiferente si el receptor realiza un acto de disposición sobre el secreto, puesto que este elemento no es indispensable para entender que el delito se ha consumado, como tampoco lo es la necesidad de que se hayan causado daños al titular del secreto. Lo verdaderamente relevante es que la revelación del contenido del secreto al tercero coloca a éste en una posición de plena disposición sobre la información revelada.

6.3. ELEMENTOS SUBJETIVOS DEL TIPO AGRAVADO

El supuesto agravado requiere al igual que sucedía con el delito común, la concurrencia de dolo. No es admisible el castigo de la conducta de revelación realizada por imprudencia, puesto que no ha sido prevista penalmente y la falta de previsión supone la atipicidad de la conducta.

El dolo en el tipo agravado requiere los elementos propios de esta figura, elementos claramente estudiados por el Tribunal

Supremo en innumerables sentencias. Entre ellas la STS 772/2004, de 16 de junio[122] entiende que

> «El dolo significa conocer y querer los elementos objetivos del tipo penal. En realidad, la voluntad de conseguir el resultado no es más que una manifestación de la modalidad más frecuente del dolo en que el autor persigue la realización de un resultado, pero no impide que puedan ser tenidas por igualmente dolorosas aquellas conductas en las que el autor quiere realizar la acción típica, representándose la posibilidad de la producción del resultado. También obra con dolo quien, conociendo que genera un peligro concreto jurídicamente desaprobado, no obstante, actúa y continúa realizando la conducta que somete a la víctima a riesgos sumamente relevantes que la gente no tiene seguridad alguna de poderlos controlar o neutralizar, sin que sea preciso que persiga directamente la causación del resultado, ya que es suficiente con que conozca que hay un elevado índice de probabilidad de que su comportamiento lo produzca».

En el delito de revelación de secretos empresariales, el dolo se materializa en la representación del resultado en la mente del autor, existiendo una conciencia por parte de éste de que con su conducta se producirá el resultado de exteriorización del secreto a terceros no autorizados para su conocimiento. Y al mismo tiempo también se requiere para que concurra el dolo en este tipo de delitos, que exista por parte del autor una voluntad clara de querer ejecutar la acción típica, por tanto, una voluntad de comunicar el secreto a los terceros no autorizados. El propio tipo agravado hace referencia en su redacción a estos terceros, con la intención clara por parte del legislador, de insistir en el hecho de que los destinatarios de la revelación han de ser personas, físicas o jurídicas, no autorizadas por el titular del secreto para su conocimiento o acceso.

---

122. TRIBUNAL SUPREMO. STS 772/2004, de 16 de junio de 2004. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/232f24a212bb84ed/20041125

Es generalmente admisible por la mayor parte de la doctrina el dolo eventual en los delitos que estudiamos. Este puede ser definido según la STS 363/2023, de 17 de mayo[123] como «conocimiento y aceptación de la posibilidad eventual, no segura, de realizar el hecho típico objetivo sin pretenderlo directamente, aceptación que se da si no hay una suficiente confianza mínimamente fundada en no producir el hecho».

Aplicando estas palabras al delito de revelación de secretos, podríamos entender que se da un supuesto de dolo eventual en aquellas ocasiones en las que el sujeto procede a la revelación a un tercero sin tener plena seguridad de si éste conoce el secreto o no. Son los supuestos como define MARTÍNEZ BUJÁN en los que se aprecia «una falta de certeza en el conocimiento del sujeto pasivo sobre el carácter reservado de la información»[124].

La conducta dolosa requiere la concurrencia y voluntad en la realización de la acción e implica también que el autor de los hechos es consciente de que con su conducta de revelación se incrementa la probabilidad de que quede lesionado el bien jurídico protegido por el precepto penal, puesto que se pone en serio riesgo el carácter secreto y exclusivo de de la información empresarial sujeta a reserva.

6.4. FORMAS IMPERFECTAS DE EJECUCIÓN DEL TIPO AGRAVADO

Dado que estamos ante un delito de resultado, como mencionábamos anteriormente, es perfectamente posible que se den las formas imperfectas de ejecución en el supuesto agravado.

---

123. TRIBUNAL SUPREMO.STS 363/2023, de 17 de mayo de 2023. Recurso electrónico disponible en:
https://www.poderjudicial.es/search/AN/openDocument/e4ff37e144938ef8a0a8778d75e36f0d/20230605

124. MARTÍNEZ-BUJÁN PÉREZ, C. *Delitos relativos al*…op., cit., p.20.

Doctrinalmente las posturas sobre las formas imperfectas del delito de revelación de secreto varían. MARTÍNEZ BUJÁN entiende, a diferencia de la doctrina mayoritaria, «que no caben formas imperfectas de ejecución y que la tentativa del tipo cualificado daría lugar siempre a una sanción menor que la que correspondería en el tipo básico.»

Por lo que respecta a la tentativa, definida en el artículo 16 del Código Penal, en el cual se dispone que « Hay tentativa cuando el sujeto da principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían producir el resultado, y sin embargo éste no se produce por causas independientes de la voluntad del autor». Es plenamente posible que el sujeto activo del delito haya procedido a la realización de uno o varios de los actos necesarios para que la información se revele, pero por circunstancias independientes totalmente de su voluntad, se frustra la revelación o no se hace posible la transmisión del conocimiento del secreto a terceras personas.

Son admisibles tanto la modalidad de tentativa acabada como de tentativa inacabada. Sería tentativa acabada la «realización de todos los actos que objetivamente deberían producir el resultado» e inacabada en el caso de que se realizaran solo esos actos parcialmente (Farre Trepat, 2011)[125].

Se daría también un supuesto de tentativa en el caso de que el autor llevara todos los actos necesarios para la revelación y ésta efectivamente se hubiera producido en favor de un tercero, pero si el tercero no adquiere como consecuencia de la revelación una situación de poder o dominio sobre la información.

La consumación del delito en su modalidad agravada se produce en aquellas ocasiones en las que el autor revela el secreto a terceros ajenos a la información, y éstos, como consecuencia de la revelación, se les coloca en tal situación con respecto al secreto, que se ven totalmente posibilitados de realizar actos de

---

125. FARRE TREPAT, E. *Tentativa del delito: doctrina y jurisprudencia.* 2011. Págs

uso, disposición o explotación del mismo. Estos actos de disposición por parte del tercero que adquiere el conocimiento del secreto no son indispensables para que el delito se entienda consumado. Basta la revelación y la puesta del secreto bajo el dominio del tercero.

Pueden darse situaciones en las cuales el tercero no adquiere un poder de dominio o disposición sobre el secreto que le ha sido revelado, como consecuencia de que el autor de los hechos en el último momento desiste de la realización de la conducta, bien de manera directa, realizando los actos necesarios para que finalmente no se produzca la revelación, o indirecta, en aquellas ocasiones en las que se limita el acceso al tercero sobre el secreto insuficientemente revelado, de forma que éste no adquiere un pleno conocimiento sobre la información. En estos supuestos resulta claro que estamos ante una situación de desistimiento[126]. Si se envía por ejemplo la información a través del correo electrónico personal del autor, y éste en el último momento lo borra, antes de que hubiera sido recibido por el tercero, supone que el auto realiza actos constitutivos de desistimiento. Como define el artículo 16.2, los actos de desistimiento son los actos tendentes «a evitar voluntariamente la consumación del delito, bien desistiendo de la ejecución ya iniciada, bien impidiendo la producción del resultado». Y son actos que aunque quedan exentos de pena, no imposibilitan el castigo de los actos que se hubieran ya ejecutado por el autor, de ser susceptibles de ser integrados en la definición de algún tipo penal.

Las conductas de revelación de secretos en grado de tentativa son castigadas de acuerdo con lo dispuesto en el artículo 62 del Código Penal, y por tanto «se impondrá la pena inferior en uno o dos grados respecto a la del delito consumado, en la extensión que se estime adecuada, atendiendo al peligro inherente al intento y al grado de ejecución alcanzado». Las conductas

126. Artículo 16 apartado 2 y 3 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Recurso electrónico disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

que conlleven un apoderamiento del secreto y una voluntad clara en su revelación, pero que por causas ajenas al autor resulten frustradas y no obtengan el resultado pretendido, serán castigadas en función de los baremos mencionados en el artículo 62. Por tanto, deberá valorarse en qué medida el interés del titular del secreto en su protección y exclusividad queda afectado por la conducta realizada por el autor, pudiendo valorarse si se han causado perjuicios efectivos al empresario titular del secreto, tanto en su rendimiento económico como en su capacidad competitiva en el mercado. También habrán de ser valorados los actos realizados por el autor, y en qué medida la realización de estos actos ha llegado a posibilitar una revelación efectiva. Los órganos jurisdiccionales tomarán estos criterios como punto de referencia a la hora de imponer la pena que consideren más conveniente para los supuestos de revelación de secretos empresariales en grado de tentativa.

6.5. AUTORÍA Y PARTICIPACIÓN EN EL SUPUESTO AGRAVADO

Son plenamente aplicables las consideraciones sobre autoría y participación que hemos realizado para el delito común de revelación de secretos. Pero en el caso del tipo agravado existe una particularidad que debemos analizar. Nos referimos a aquellos casos en los cuales el tercero receptor del secreto ha podido participar de alguna manera en la realización de la conducta, colaborando con el autor para que la revelación se produzca. La necesidad de que concurra no sólo un acto de revelación por parte del autor, sino una puesta a disposición del tercero receptor del contenido del secreto, de tal forma que éste adquiera algún tipo de poder o control sobre la información revelada para que el tipo agravado se entienda consumado, ha propiciado que la doctrina califique el delito como un delito pluripersonal o plurisubjetivo. Así por ejemplo CARRASCO ANDRINO, entiende que «la pluripersonalidad determina la perfección o consumación del delito, dando lugar la actuación de un

solo sujeto a una tentativa punible, sin que la del otro sea necesaria.» (Carrasco Andrino, 1998).[127]

«Sin duda alguna el delito de revelación de secretos empresariales requiere la concurrencia de dos voluntades, la del autor de revelar el hecho al tercero, y la del tercero en adquirir el conocimiento al que no se encuentra autorizado. Ambas conductas son indispensables para que su tipo agravado se produzca, y ambas conductas afectan al bien jurídico protegido de manera directa.»

Pero lo cierto es que el tercero que recibe el secreto, por haberle sido revelado por el autor del delito agravado, no es necesario que conozca el contenido de la información, o incluso que la comprenda. Es suficiente con que se le coloque en tal situación de control sobre el secreto, que aún no conociendo su contenido o no comprendiéndolo, pueda disponer y usar de él en su beneficio o en el de un tercero, quebrando los derechos de protección del empresario.

El hecho de que los delitos pluripersonales requieran que las dos partes activas que realizan la conducta tengan conciencia del riesgo para el bien jurídico protegido y de la posible lesividad derivada de su actuación es lo que motiva la consideración como delito plurisubjetivo. Pero esta conciencia, en el caso del delito de revelación de secretos, no parece susceptible de ser exigida para el tercero a quien se le revela el secreto. Sí es necesario para la consumación del delito que el tercero adquiera la situación de dominio que comentábamos, pero no que exista una voluntad o una consciencia clara de la lesividad del bien jurídico protegido. Cualquier situación en la que el tercero receptor colabore de alguna manera con el autor del delito de revelación, para que efectivamente ésta pueda producirse, no puede ser entendida como un supuesto de participación necesaria, porque a veces esa participación es nimia, y consistente en actos de escasa importancia, que no reflejan una voluntad por parte del tercero en participar en la comisión del delito. Puede tratarse de actos meramente co-

---

127. CARRASCO ANDRINO, M. *La protección penal del....* Op., Cit., p.20.

laborativos que se realicen sin tener conciencia de que su participación contribuye a la producción del resultado. Actos que realmente tienen una importancia accesoria o irrelevante, puesto que no son indispensables para la comisión del delito de revelación. Lógicamente si el tercero participa en la comisión del delito realizando actos que inevitablemente conducen a la producción del resultado, siendo consciente de que con su conducta se producirá la revelación, si estaríamos ante un supuesto de coautoría o complicidad.

La STS 1379/2021, de 15 de abril[128] trata la materia de manera clara.

> «La intervención del cooperador necesario mantiene una estructura accesoria del delito principal. Las exigencias están orientadas a que el hecho del autor principal sea típico, antijurídico y doloroso, de acuerdo con la teoría de la accessoriedad limitada. No es suficiente con que la autora haya realizado una acción antijurídica. El fundamento de la responsabilidad del participio no es ajeno al carácter injusto del hecho por el autor, y es necesario que el autor actúe dolorosamente o con previsibilidad objetiva de la posibilidad de realizar el tipo objetivo. En consecuencia, el desconocimiento por parte del autor de las circunstancias objetivas y subjetivas del tipo nos satisface el juicio de antijuridicidad y resulta insuficiente para justificar la punibilidad del partícipe.»

Es plenamente aplicable al tipo agravado de revelación de secretos lo dispuesto sobre participación y coautoría por el Tribunal Supremo. De su doctrina al respecto destaquemos la STS 623/2015, de 13 de octubre de 2015[129]

---

128. TRIBUNAL SUPREMO. STS 1379/2021, de 15 de abril de 2021. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/8244db7a8797ee08/20210428

129. TRIBUNAL SUPREMO. STS 623/2015, de 13 de octubre de 2015. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/3361dfa7cdd02121/20151109

«La jurisprudencia de esta Sala tiene declarado que, en los delitos dolosos, la común responsabilidad de los partícipes se basa en el acuerdo entre los distintos intervinientes en la acción, pero sustancialmente en la ejecución de un reparto de papeles con aportaciones causales recíprocas que dan lugar a lo que se ha denominado la imputación conjunta o recíproca de la acción.

Esta Sala ha valorado la concurrencia de los siguientes elementos:

1) Que alguien hubiera dado comienzo a la ejecución del delito.

2) Que posteriormente otro u otros ensamblen su actividad a la del primero para lograr la consumación del delito cuya ejecución había sido iniciada por aquél.

3) Que quienes intervengan con posterioridad ratifiquen lo ya realizado por quien comenzó la ejecución del delito aprovechándose de la situación previamente creada por éste, no bastando el simple conocimiento.

4) Que cuando intervengan los que no hubieran concurrido a los actos de iniciación ya no se hubiese producido la consumación, puesto que, quien interviene después, no puede decirse que haya tomado parte en la ejecución del hecho;

5) que la coautoría presupone la común y unitaria resolución de todos los partícipes para llevarla a efecto, siendo esencial la unidad de conocimiento y voluntad de aquéllos como elemento subjetivo, junto al objetivo de la puesta en práctica de la acción conjunta, debiendo tener la actuación de cada uno la entidad y relevancia precisas que definan al delito;

6) que la coautoría debe ir acompañada en su vertiente subjetiva por dolo directo o eventual; que el acuerdo de voluntades entre dos o más personas para llevar a efecto la realización de un plan delictivo por ellos trazado, establece entre los que se conciertan un vínculo de solidaridad penal que les hace partícipes con igual grado de responsabilidad, cualquiera que sea la función o cometido que a cada uno de los concertados se le asigne; y

7) que la jurisprudencia actual rompe con la idea de que la existencia de un acuerdo previo convierte a los diversos partícipes en coautores, pues conllevaría a un criterio extensivo de autor y calificaría como tal a toda forma de participación concertada, sin tener en cuenta el aporte objetivamente realizado al delito. Por este motivo, la jurisprudencia se ha acercado cada vez más a un concep-

> to de autoría fundado en la noción del dominio del hecho, para el que resulta decisivo, en relación a la determinación de si se ha «tomado parte directa» en la realización de la acción típica, la posición ocupada por el partícipe en la ejecución del hecho.»
>
> «Toda participación en la comisión del hecho delictivo —para implicar una responsabilidad criminal— ha de ser consciente y querida. Es lo que constituye el elemento subjetivo de la coautoría. El otro elemento —el objetivo—, se concreta en la ejecución conjunta del hecho criminal.»

Hacemos mención literal de estos fragmentos de la sentencia por considerarlos esenciales a la hora de diferenciar las conductas de coautoría y participación y porque siendo difícil la delimitación de tales figuras en el tipo agravado de revelación de secretos del artículo 278.2, al igual que sucedía en el delito común, entendemos que podrán aportar luz al respecto.

7. Las conductas del Artículo 279 y 280 del Código Penal

El artículo 279 del Código Penal típica la siguiente conducta.

> «La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
>
> Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior.»

Las conductas contempladas en el artículo 279 son básicamente las mismas previstas en el tipo básico del artículo 278. Consisten en la difusión, revelación o cesión de un secreto de empresa. Por tanto, todas las consideraciones que al respecto hemos hecho en las páginas anteriores, cuando analizábamos qué diferenciación podría existir entre los términos utilizados por el legislador penal son plenamente aplicables a las conductas previstas en el artículo 279.

El elemento diferencial radica en quién pueda ser considerado sujeto activo del delito, puesto que las conductas a las que se refiere requieren que sean realizadas por aquella persona «que tuviere legal o contractualmente obligación de guardar reserva». Sin perjuicio de que la cuestión haya sido analizada de forma amplia por la jurisprudencia ordinaria, son especialmente esclarecedoras las resoluciones del Tribunal Supremo. En concreto la STS 258/2008, de 12 de mayo, pues en ella se hace

una identificación clara de quiénes pueden cometer el delito y la STS 285/2008, de 12 de mayo que aporta una visión esclarecedora de los supuestos en los que la obligación de reserva recae sobre los trabajadores.-

La violación de secretos contemplada en el artículo 13 de la Ley de Competencia Desleal se considera una conducta desleal. Este precepto, que abarca tres tipos de conductas diferentes, ha representado una mejora técnica significativa en comparación con la regulación previa contenida en el artículo 499 del Código Penal de 1973. Esta mejora amplía considerablemente el ámbito de aplicación respecto al sujeto activo.

En primer lugar, al no limitarse a los «encargados, empleados u obreros», la norma incluye también a los miembros del consejo de administración de la empresa, así como a otros administradores y directivos que difícilmente encajaban en la categoría de «empleados». En segundo lugar, la conducta también se extiende a personas sin relación de dependencia con la empresa titular del secreto, pero que, debido a obligaciones contractuales o legales, están obligadas a mantener la confidencialidad de la información a la que tienen acceso.

Finalmente, de manera especialmente relevante, la regulación actual contempla la posibilidad de que quienes han cesado su relación con la empresa puedan cometer este tipo de infracción, algo que antes no era posible según la interpretación mayoritaria de la doctrina, como lo señala PACHECO[130].

Los sujetos activos del delito contemplado en el artículo 279 son aquellos a los que son susceptibles de serle exigida confidencialidad y reserva en el ámbito de sus relaciones laborales o profesionales. Así por ejemplo, podríamos entender incluidos a los administradores, los trabajadores con obligación de confidencialidad, los representantes legales de los trabajadores que suelen tener acceso a información empresarial relevante susceptible de ser considerada como secreto de empresa, los ase-

130. CUERDA ARANAU, M.L. Comentarios al Código Penal (2 tomos). Valencia. 2023. Página 1.746

sores de los representantes legales de los trabajadores que participan en las mesas negociadoras y tienen posibilidad, en el desarrollo de la negociación, de tener conocimiento de secretos susceptibles de ser calificados como de empresa. Pero también podríamos entender que son susceptibles de ser considerados autores del delito, los trabajadores de otras empresas distintas de aquella titular del secreto, pero que entablan con ésta algún tipo de relación o prestación de servicios (como por ejemplo serían proveedores, asesorías, asesores en seguridad informática, etc). Estas personas susceptibles de ser consideradas autoras del delito de revelación del artículo 279 también ha sido contempladas por la jurisprudencia en sentencia AAP Castellón, a 28 de febrero de 2022[131] que dispone que:

> «El delito del art. 278, como se ha visto ha declarado el Tribunal Supremo, no es un delito especial pero sí exige que quien accede al secreto no lo conozca ya, lo que le diferencia del art. 279, este sí es un delito especial, como ha recordado la sentencia 285/2008 de 12 de mayo por cuanto solo lo pueden cometer aquellos a «quienes se les exige expresamente (administradores, ex art.127.2 LSA y 61.2 LRL), al resto de empleados de la empresa que conozcan por razón de sus funciones tales secretos, a trabajadores de otras empresas que se relacionen con la titular de los secretos (de seguridad, proveedoras, etc.), y a los terceros que los hayan conocido a causa de razones legales (como, por ejemplo, funcionarios). Y como «delito especial propio», sólo pueden cometerlo el círculo de personas indicadas, respondiendo, en su caso, el «extraneus», como cooperador (inductor, cooperador necesario, cómplice) según en qué haya consistido su participación», en el cual quien difunde el dato o datos que han de permanecer ocultos los conoce y la difusión se produce con el fin de obtener un beneficio propio.»

---

131. AUDIENCIA PROVINCIAL DE CASTELLÓN. SAP Castellón 118/2022, de 28 de febrero de 2022. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/435fd1c6dfc89317a0a8778d75e36f0d/20231227

La STS 864/2008, 16 de diciembre de 2008[132] nos aclara para el artículo 279 que:

> «Sujeto activo ha de ser quien tuviere legal o contractualmente obligación de guardar reserva, esto es, de mantener el secreto que él precisamente conoce porque su relación concreta con la empresa así lo exige. Se trata como ya se ha dicho, no de un delito común, como el del 278, sino de un delito especial propio.

La STS 285/2008 a 12 de mayo de 2008[133] delimita a los posibles autores pues:

> «Como más arriba dijimos, el fundamento del castigo se encuentra en la lealtad que deben guardar quienes conozcan el secreto, por su relación legal o contractual con la empresa, ya que el bien, específicamente tutelado, consistirá en la competencia leal entre las empresas.

Pero la sentencia citada es también esencial para delimitar el artículo 279 en materia de dolo y error.

> «El tipo del art. 279 aplicado, se caracteriza por la infracción de un deber extrapenal específico de guardar secreto que, -según entiende la doctrina- independientemente de la eventual cláusula de duración contractual determinada, se encuentra vigente, respecto de las personas que cesan en la empresa, mientras esté en condiciones de aportar un valor económico.»
>
> «En quinto lugar, es cierto que la figura penal aplicada, como delito de tendencia que es (Cfr. STS nº 1607/2000, de 16 de febrero),

---

132. TRIBUNAL SUPREMO. STS 864/2008, de 16 de diciembre de 2008. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/ca4dddcef35a60e6/20090219

133. TRIBUNAL SUPREMO. STS 285/2008 de 12 de mayo de 2008. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703

requiere dolo, y por ello es concebible el error, especialmente sobre el deber de especial sigilo, cuando el sujeto cree que ha terminado tal obligación..

Una de las cuestiones que plantea del artículo 279 es la necesidad de diferenciar el secreto empresarial del denominado «*skill and knowledge*» (Antón y Abajo, 2023). Este término anglosajón hace referencia a los conocimientos y habilidades que un trabajador adquiere como consecuencia de prestar sus funciones en la empresa. Las conductas de revelación de secretos de empresa no pueden entenderse cometidas en el caso de que el objeto de revelación sean las meras capacidades y conocimientos adquiridos por el trabajador en el desempeño de sus funciones, pues se requiere que el objeto de la revelación sean los secretos de empresa.

Es decir, La cuestión más compleja del precepto radica en la duración y el alcance del deber de confidencialidad una vez finalizada la relación con la empresa. El principal punto de debate es determinar si dicho deber debe estar recogido en una norma legal o en una cláusula contractual específica, o si basta con un deber genérico basado en la buena fe y la diligencia debida. Esta última opción parece poco viable, ya que situaría la imputación en la creación o aumento de un riesgo no permitido, en lugar de fundamentarse en la violación de una obligación concreta[134].

En cuanto al periodo durante el cual debe mantenerse el deber de confidencialidad cuando no está estipulado en la normativa o en un contrato, la doctrina ofrece diferentes enfoques. Algunos sostienen que podría aplicarse el plazo máximo de dos años previsto en el artículo 21.3 del Estatuto de los Trabajadores para los pactos de no competencia, mientras que otros se inclinan por considerar la adecuación social de la conducta. La jurisprudencia, por su parte, ha establecido que el deber de secreto se extiende también a quienes ya no forman parte de la

134. CUERDA ARANAU, M.L. Comentarios al Código Penal…Op., cit., página 1.747

empresa, siempre que la información siga teniendo un valor económico[135].

La STS 446/2008 de 29 de mayo[136] considera que los trabajadores y todos aquellos que de una y otra manera colaboran o prestan sus servicios profesionales con el empresario titular del secreto tienen pleno derecho a utilizar, en plena libertad, todos aquellos conocimientos y capacidades que hubieran adquirido como consecuencia de haber prestado sus servicios en la empresa. La STS 1169/2006, de 24 de noviembre[137] que señala que «no pueden ser objeto de secreto empresarial aquellas informaciones que forman parte de las habilidades, capacidades y experiencia profesionales de carácter general de un sujeto, ni tampoco el conocimiento y relaciones que pueda tener con la clientela, aun cuando dichas habilidades o capacidades se hayan adquirido en el desempeño de un puesto determinado o de unas concretas funciones desarrolladas para un determinado empleador.»

Todo aquel trabajador que está sujeto a una obligación de reserva en el desempeño de su puesto de trabajo, adquiere al igual que cualquier otro trabajador no sujeto a tal reserva, una serie de conocimientos técnicos y profesionales. El trabajador tiene derecho a que estos conocimientos sean utilizados y revelados, e incluso que disfrute de tales conocimientos el futuro empresario que lo contrate una vez haya finalizado la relación laboral con la empresa en la que ha prestado sus servicios.

Sólo pueden entenderse incluidas en las conductas de difusión, revelación y cesión por quien tenga obligación de reserva, aquellas ocasiones en las que los trabajadores revelan informaciones susceptibles de ser consideradas como secretos de empresa

---

135. TRIBUNAL SUPREMO. STS 285/2008, de 12 de mayo.

136. TRIBUNAL SUPREMO. STS 446/2008 de 29 de mayo de 2008. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/eff2c6a56f7a2e2c/20080730

137. TRIBUNAL SUPREMO. STS 1169/2006, de 24 de noviembre de 2006. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/92f25837fb00abf3/20061228

Suele ser bastante frecuente que las empresas especialmente interesadas en salvaguardar su información y protegerla frente a un inadecuado conocimiento por parte de su competencia obliguen a los trabajadores a firmar cláusulas de confidencialidad para intentar de esta manera proteger la información sensible de la empresa. Es frecuente que estas cláusulas fijen un periodo de tiempo limitado, pero lo cierto es que las cláusulas de confidencialidad vinculan a los trabajadores incluso después de que haya finalizado su relación laboral. Es posible que habiéndose realizado una conducta de revelación de información sensible por parte del trabajador con obligación de reserva una finalizada el contrato laboral, no sólo el trabajador puede ser castigado como autor de un delito del artículo 279, sino que la empresa puede solicitar una indemnización de daños y perjuicios por la vía civil. Es indispensable probar el perjuicio para la empresa y que la revelación se ha llevado a cabo infringiendo el deber de reserva.

La obligación de guardar reserva es un deber básico del trabajador, cuando en virtud de su contrato de trabajo se haya obligado a no difundir o revelar informaciones o secretos empresariales de los que haya tenido conocimiento. El «Estatuto de los Trabajadores aprobado por Real Decreto Legislativo 2/2015 de 23 octubre», lo contempla en el artículo 5.a). Hace Referencia de forma indirecta a este deber de confidencialidad al establecer que «los trabajadores tienen como deberes básicos: a) cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia».

Si dentro de los términos del contrato de trabajo se incluyen cláusulas de confidencialidad, el trabajador se ve el ineludiblemente obligado a su cumplimiento. De hecho, como se dispone en el artículo 20 del Estatuto de los Trabajadores, a efectos de garantizar el cumplimiento del deber de guardar reserva, «el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración de vida a su digni-

dad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.»

También a las conductas de revelación de secretos por parte de aquellos que tengan obligación de reserva alude el artículo 3 de la «Ley de secretos empresariales 1/2019», concretamente en su apartado dos, al disponer lo siguiente:

> «La utilización o revelación de un secreto empresarial se consideran ilícitas cuando, sin el consentimiento de su titular, la realice quien haya obtenido el secreto empresarial de forma ilícita, quien haya incumplido un acuerdo de confidencialidad o cualquier otra obligación de no revelar el secreto empresarial, o quien haya incumplido una obligación contractual o de cualquier otra índole que limite la utilización del secreto empresarial».

A nivel jurisprudencial, la STS 285/2008 a 12 de mayo de 2008[138]:

> «El Real Decreto Legislativo 1/95, de 24 de marzo, que aprobó el texto refundido del Estatuto de los Trabajadores, dispone en su art. 5 que son deberes laborales del trabajador: d) No concurrir con la actividad de la empresa en los términos fijados en esta Ley; precisando el art. 21.2 que el pacto de no competencia para después de extinguido el contrato de trabajo, que no podrá tener una duración superior a dos años para los técnicos y de seis meses para los demás trabajadores, sólo será válido si concurren los requisitos siguientes: a) Que el empresario tenga un efectivo interés industrial o comercial en ello, y b) Que se satisfaga al trabajador una compensación económica adecuada.»

La figura descrita en el segundo párrafo se configura como un tipo atenuado o privilegiado, dependiente del tipo básico, por lo que las consideraciones relativas al sujeto activo y al ob-

---

138. TRIBUNAL SUPREMO. STS 2885/2008 de 12 de mayo de 2008. Recurso electrónico disponible en: https://www.poderjudicial.es/search/AN/openDocument/278e7ab325928481/20080703

jeto material también le son aplicables. Esta disposición constituye una novedad significativa respecto al Código Penal de 1973, cuya regulación impedía que se considerara delito el uso de un secreto en beneficio propio, como lo establecía la antigua jurisprudencia[139]. Aunque no se cuestiona la corrección de esta reforma punitiva, sí genera debate la justificación de la atenuación de la pena, que resulta difícil de defender desde un punto de vista lógico y jurídico.

En cuanto a lo dispuesto en el artículo 280, el precepto sanciona la divulgación de secretos empresariales por parte de terceros, estructurándose de manera similar al párrafo segundo del artículo 197.3 del Código Penal. Al igual que este, el tipo delictivo presenta un elemento positivo, que es el conocimiento del origen ilícito de la información, y un elemento negativo, que consiste en la ausencia de participación en la obtención del secreto.

En el artículo 280 se tipifica la conducta del que conoce el origen ilícito de la información y sin participar en el descubrimiento, procede a apoderarse de los soportes, datos o documentos constitutivos de secreto (artículo 278) o a la difusión, revelación o cesión de secreto empresarial (artículo 279). El tenor literal del precepto dice «El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses.»

En relación con el segundo elemento negativo previamente mencionado, se presenta un problema interpretativo significativo del precepto, ya que dificulta cumplir literalmente con la referencia a la realización de «alguna de las conductas descritas en los dos artículos anteriores». En realidad, el sujeto activo únicamente puede llevar a cabo las conductas descritas en los artículos 278.2 y 279, dado que el artículo 278.1 se refiere específicamente al descubrimiento del secreto.

---

139. TRIBUNAL SUPREMO. STS de 4 de abril de 1972

En cuanto al elemento positivo, en principio, se podría limitar a los casos de acceso ilícito, es decir, los contemplados en el artículo 278.1, dado que el artículo 279 parte del conocimiento lícito por parte del sujeto. Sin embargo, esta interpretación debe ser rechazada. El concepto de «origen ilícito» debe entenderse de manera más amplia, incluyendo también los comportamientos descritos en el artículo 279. La ilicitud no debe centrarse únicamente en la forma de acceso, sino en la violación de los deberes de confidencialidad impuestos al poseedor del secreto empresarial. Esto no solo evita un trato diferencial injustificado a comportamientos con el mismo desvalor, sino que también garantiza la aplicabilidad del precepto, al descartar la remisión exclusiva a la conducta del artículo 278.1[140].

De nuevo la relevante STS 864/2008, de 16 de diciembre nos da las claves para delimitar el artículo 280 pues nos recuerda que son elementos del tipo necesario para entender la conducta realizada el «no haber tomado parte en el descubrimiento de secreto» y «actuar con conocimiento del origen ilícito de ese descubrimiento»

Estos dos son los elementos que determinan la aplicabilidad el artículo 280. La remisión del precepto «a las conductas descritas en los dos artículos anteriores» nos permite extrapolar todo lo que hemos dicho en materia de autoría, participación, conceptualización de secreto de empresa y diferenciación entre difusión revelación y cesión. Nos remitimos pues a lo anteriormente dicho.

Sí debemos hacer mención de que el autor, para poder ser considerado como tal, debe conocer el origen ilícito de la información. Cualquier persona que haya participado en la realización de las conductas necesarias para la obtención del secreto, pero que no haya participado de forma directa en la revelación de este, serán castigadas como partícipes, cooperadores necesarios o cómplices, pero no serán susceptibles de ser califica-

---

140. CUERDA ARANAU, M.L. Comentarios al Código Penal…Op., cit., Página 1749

dos como autores del tipo previsto en el artículo 280. Por lo demás, el precepto apenas presenta especificidades, siéndole aplicable lo anteriormente estudiado en páginas anteriores al tratar los artículos 278 y 279 y las conductas típicas en estos preceptos recogidas.

No obstante, la doctrina ha debatido si el conocimiento requerido para el tipo penal presupone dolo directo o si es suficiente con dolo eventual. Aunque algunos autores abogan por exigir dolo directo, el dolo eventual no puede descartarse, ya que es compatible con la estructura del tipo penal y con la redacción legal utilizada. Además, existen razones de política criminal que justifican aceptar el dolo eventual para evitar una brecha significativa en la impunidad[141].

Desde el punto de vista subjetivo, no es necesario que el sujeto tenga un conocimiento exacto del delito subyacente. Bastará con que esté consciente de la irregularidad de la situación y pueda inferir razonablemente que esta proviene de un acto delictivo. Esto es aplicable a casos en los que el sujeto se encuentra en una posición de «ignorancia deliberada»[142], «mera indiferencia»[143] o «ceguera voluntaria»[144], que son supuestos de dolo eventual.

Se dará lugar a un concurso de normas cuando una persona que haya participado en los delitos descritos en los artículos 278.2 y 279 cometa adicionalmente la conducta tipificada en el artículo 280. En tal caso, la resolución deberá aplicar el artículo 280 conforme a las reglas 1ª y 4ª del artículo 8 del Código Penal.

---

141. CUERDA ARANAU, M.L. Comentarios al Código Penal…Op., cit., Página 1750
142. TRIBUNAL SUPREMO. STS 126/2007, de 5 de febrero.
143. TRIBUNAL SUPREMO. STS 359/2008 de 19 de junio.
144. TRIBUNAL SUPREMO. STS 129/2011, de 10 de marzo.

8. Reflexiones sobre las lagunas punitivas del Artículo 200 del Código Penal

Conviene finalizar haciendo alusión a las lagunas punitivas del artículo 200 del Código Penal en relación con los artículos que se acaban de analizar. Es importante destacar que, aunque se han discutido diversos aspectos de la legislación vigente, persisten áreas que requieren atención y revisión para garantizar una adecuada protección legal. Las similitudes entre las modalidades comisivas y la estructura típica de los delitos relacionados con la violación de secretos empresariales y los delitos de descubrimiento y revelación de secretos personales no ocultan la existencia de ciertas lagunas punitivas difíciles de justificar, lo que podría llevar a situaciones de impunidad en ciertos casos específicos.

En primer lugar, se observa una carencia notable en la regulación de conductas relacionadas con el abuso informático, tales como la alteración y modificación de información reservada contenida en redes o soportes informáticos. Mientras el artículo 197.2 del Código Penal aborda estos actos dentro del contexto de secretos personales, el artículo 278 se limita a los actos de espionaje industrial, excluyendo específicamente estas formas de manipulación informática que pueden tener consecuencias graves para la privacidad y la seguridad de la información. Las conductas relacionadas con el vandalismo electrónico o *cracking* deberían ser contempladas en los artículos 264 y 264 bis del Código Penal, que regulan el sabotaje informático entre los delitos de daños. Sin embargo, es relevante señalar que estas

conductas no están necesariamente motivadas por el objetivo de menoscabar la competitividad de una empresa o de obtener una ventaja competitiva, lo que plantea un vacío en la cobertura punitiva para tales actos, dejando desprotegidos a muchos individuos y organizaciones que podrían ser víctimas de estas acciones ilícitas.

Del mismo modo, en la revisión de los artículos 278 y siguientes del Código Penal, se observa que no se ha incluido la modalidad agravada que se encuentra estipulada en el artículo 197.4. Esta modalidad agravada se aplica específicamente a aquellas personas que tienen la responsabilidad o el encargo de gestionar ficheros, soportes informáticos, electrónicos o telemáticos, así como archivos o registros. La importancia de esta omisión radica en que la mayor reprochabilidad que se asocia a estas conductas se extiende también a los actos que implican la violación de secretos empresariales, lo que podría tener implicaciones significativas en el ámbito de la protección de la información sensible en el entorno corporativo.

Además, es relevante mencionar que la posibilidad de sancionar algunas de las conductas que han sido excluidas de la regulación de los artículos 278, 279 y 280 se puede encontrar en el artículo 200 del mismo Código Penal. Este artículo establece que «lo dispuesto en este capítulo será aplicable al que descubra, revele o ceda datos reservados de personas jurídicas sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos del Código». La interpretación de este artículo 200 presenta ciertas complejidades y no resulta sencilla. En un enfoque restrictivo, se podría argumentar que los datos reservados mencionados en el artículo 200 son aquellos cuya relevancia empresarial se encuentra bajo la custodia de personas físicas, las cuales ya están protegidas por los artículos 278, 279 y 280 del Código Penal, que tendrían una aplicación preferente en estos casos.

No obstante, el precepto del artículo 200 parece estar dirigido de manera específica a la protección de datos reservados de personas jurídicas. Esto sugiere que, en el caso de que el objetivo fuera sancionar la revelación de datos de personas físicas

que son custodiados por entidades jurídicas, la existencia del artículo 200 podría no ser necesaria. Esta distinción es crucial para entender cómo se aplican las sanciones y las responsabilidades en el contexto de la protección de datos y secretos empresariales, así como para evaluar la efectividad de la legislación vigente en la materia.

Ambas interpretaciones, que se han presentado en el contexto del análisis jurídico, rompen con la clara distinción que normalmente se establece entre los diferentes bienes jurídicos que son protegidos por cada grupo de delitos. Es importante señalar que esta ruptura no solo afecta a la clasificación de los delitos, sino que también tiene implicaciones significativas en la aplicación de la ley. Además, es fundamental no olvidar que los conceptos de persona jurídica y empresa no son equivalentes, aunque a menudo se utilicen de manera intercambiable en el discurso cotidiano. Esta confusión puede llevar a malentendidos en la interpretación de las normas legales.

En consecuencia, el artículo 200 del Código Penal, que se refiere a ciertas disposiciones legales, no puede subsanar las posibles lagunas típicas que se encuentran en los artículos 278, 279 y 280.

Estos artículos están relacionados con la regulación más protectora de los delitos que se incluyen en el Capítulo I del Título X del mismo código. Es crucial entender que esta situación no es simplemente un error o una omisión, sino que responde a una decisión legislativa deliberada que ha sido tomada por el legislador. Esta decisión no puede ser corregida a través de la interpretación sin vulnerar el principio de tipicidad penal, que es un pilar fundamental del derecho penal, garantizando que las conductas sean claramente definidas y tipificadas antes de que se pueda aplicar una sanción.

9. Caso práctico real: la STS 735/2024[145]

Para tratar de explicar de manera práctica todo lo mencionado a lo largo de este trabajo, se procede a analizar un caso real y reciente del año 2024, que culminó con una sentencia del Tribunal Supremo, fijando así todos y cada uno de los elementos del delito.

En el análisis del caso STS 735/2024, el Tribunal Supremo se pronuncia sobre un delito de revelación de secretos empresariales regulado en el artículo 278 del Código Penal. El caso involucra a Eduardo, un antiguo trabajador contratado como informático para desarrollar una página web para la empresa DIRECCION001. Aprovechando esta posición, Eduardo accedió sin autorización a información confidencial, incluyendo listados de clientes, balances financieros y otros datos clave de la empresa. Posteriormente, ofreció esta información a una empresa competidora, 360 DH, SL, a cambio de 1.500 euros.

El Tribunal Supremo mantiene la condena impuesta a Eduardo por el delito de descubrimiento y revelación de secretos empresariales. Como ya se ha puesto de manifiesto con anterioridad, este delito se tipifica cuando una persona se apodera de datos, documentos o cualquier tipo de soporte que contenga información confidencial de una empresa con el fin

145. TRIBUNAL SUPREMO. STS 735/2024 de 12 de julio de 2024.

de descubrirla y, en el caso agravado del artículo 278.2, cuando esta información se revela o cede a terceros.

El acusado se apoderó de la información de DIRECCION001 utilizando su posición de confianza dentro de la empresa. Aunque había finalizado su relación laboral años antes, Eduardo retuvo acceso a información sensible y la ofreció a una empresa competidora. El Tribunal consideró que este acto constituye una violación directa del secreto empresarial.

El Tribunal analiza en profundidad la aplicación del artículo 278 del Código Penal, que protege los secretos empresariales en el ámbito del derecho penal. Dicho precepto, como ya se ha mencionado con anterioridad, contempla tanto el descubrimiento ilícito de secretos empresariales (artículo 278.1) como su revelación o difusión (artículo 278.2), siendo este último el más grave debido a las implicaciones que tiene para la competencia leal en el mercado.

En este caso, se cumplen los elementos del delito:

Obtención ilícita de información: Eduardo accedió sin autorización a listados de clientes, datos financieros y otros documentos empresariales confidenciales.

Finalidad de lucrarse: La conducta del acusado no solo consistió en descubrir el secreto empresarial, sino que buscaba beneficiarse económicamente al ofrecer la información a una empresa competidora por 1.500 euros.

Revelación de secretos: El acusado hizo efectivo el ofrecimiento de la información a la empresa competidora, cumpliendo con el agravante del artículo 278.2, al intentar ceder la información comercial de DIRECCION001.

En el análisis, el Tribunal subraya que el bien jurídico protegido en este tipo de delitos es la capacidad competitiva de la empresa afectada. El acceso ilícito a datos como los listados de clientes o balances económicos representa una vulneración significativa del derecho a la libertad de empresa y al desarrollo empresarial en un entorno competitivo.

Este tipo de conductas afecta no solo a los intereses patrimoniales de la empresa, sino también al orden económico y a la competencia leal en el mercado, tal como se ha expuesto en

el análisis doctrinal de este delito. Así, el derecho penal actúa como un mecanismo protector no solo de los derechos individuales de las empresas, sino también del correcto funcionamiento del mercado.

El Tribunal, finalmente, confirmó la pena impuesta en instancias anteriores de tres años de prisión y una multa de doce meses por la violación de secretos empresariales. Además, la sentencia establece que la mera oferta de la información a una empresa competidora ya constituye un acto de revelación del secreto empresarial, por lo que no era necesario que la empresa competidora hiciera uso de la información ofrecida para que se consumara el delito.

La sentencia también reconoce la existencia de una atenuante de dilaciones indebidas, debido a retrasos procesales ajenos al acusado, lo que conllevó una reducción en la condena original.

Este caso ilustra claramente la gravedad del delito de revelación de secretos empresariales y la severidad con la que los tribunales españoles abordan este tipo de infracciones. La protección de la información confidencial en el ámbito empresarial es esencial para garantizar un entorno de competencia justa y leal. Asimismo, se evidencia la necesidad de que las empresas implementen medidas de seguridad adecuadas para salvaguardar su información sensible, tal como se ha destacado en el desarrollo de este trabajo.

Tras el resumen del caso, se procede a plasmar los aspectos más relevantes del asunto tal y como se recogen en la sentencia mencionada.

El Juzgado de Instrucción nº2 de Fuenlabrada instruyó las Diligencias Previas 893/2017 contra Eduardo, por delito de descubrimiento y revelación de secretos en el ámbito empresarial. Una vez concluido el proceso, lo remitió al Juzgado de lo Penal nº3 de Móstoles, que en el Procedimiento Abreviado nº 220/2019, dictó la sentencia nº 86/2020, de fecha 31 de enero de 2020, la cual contiene los siguientes hechos probados:

— Eduardo era mayor de edad, nacido en China con nacionalidad española y sin antecedentes penales. En el año

2005, Eduardo realizó trabajos como informático, diseñando la página web para la empresa DIRECCION000. Aprovechó esta circunstancia para obtener, sin autorización, diversa información confidencial relativa a la situación financiera de dicha empresa, sus facturas y balances, así como los listados de sus clientes.

— En el mes de julio del año 2017, el acusado ofreció esta información comercial de la empresa DIRECCION001, en particular su listado de clientes, a otra empresa denominada 360 DH, S.L., dedicada a la misma actividad comercial. Llegó a mostrarles el contenido de esta información y solicitó a cambio la cantidad de 1.500 euros. Los responsables de la empresa 360 DH, S.L. sospecharon que el acusado pudiera haber obtenido esta información de forma ilícita, por lo que lo pusieron en conocimiento de la empresa DIRECCION001, cuyo propietario, Ismael, decidió denunciarlo.

— En la tarde del día 20 de julio de 2017, agentes del Cuerpo Nacional de Policía detuvieron al acusado cuando se encontraba en las inmediaciones de la empresa 360 DH, SL. El arresto se produjo justo cuando el acusado estaba a punto de hacer entrega de información comercial de la empresa DIRECCION001. Dicha información estaba almacenada en un *Pen Drive* de la marca EMTEC. Este dispositivo de almacenamiento portátil fue incautado por la policía en el momento de la detención. Los agentes procedieron a revisar el contenido del *Pen Drive*, encontrando múltiples archivos y documentos que contenían información sensible y confidencial de la empresa DIRECCION001.

— Previa autorización judicial acordada mediante auto de fecha 8 de septiembre de 2018 por el Juzgado de Instrucción nº 2 de Fuenlabrada, se procedió al examen de este dispositivo, hallando almacenado en él una carpeta denominada «DIRECCION001» que tenía 5 carpetas en su interior con las siguientes denominaciones y contenido: Carpeta denominada «FACTURAS» con un fichero com-

primido RAR que contenía diversos archivos de facturas de esa empresa y un archivo en formato PDF de otra factura. Carpeta denominada «JPG» que almacenaba un archivo de imagen llamado DIRECCION001 1 correspondiente a un pantallazo realizado a dos mensajes de correo electrónico DIRECCION002. Carpeta denominada «LISTA DE CLIENTES» que almacenaba dos ficheros, uno de ellos en formato Excel que contenía el listado de los clientes de la empresa DIRECCION001 con nombre y apellidos, así como su teléfono y el email de contacto de su empresa. Carpeta denominada «RESUMEN VENTAS» que tenía almacenados diferentes archivos en los que obran el balance de la empresa DIRECCION001, ventas realizadas e información financiera de la misma. Carpeta denominada «SQL» que contenía dos ficheros denominados EQUIPAMIENTO COMERCIAL.

Posteriormente, el Juzgado de lo Penal nº3 de Móstoles dictó el siguiente pronunciamiento:

> «escubrimiento y revelación de secretos empresariales del artículo 278.1 y 2 del Código Penal, sin que concurran circunstancias modificativas de la responsabilidad penal, a la pena de tres años de prisión, inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de condena y multa de doce meses a razón de diez euros por día con responsabilidad personal subsidiaria para caso de impago de un día de privación de libertad por cada dos cuotas no pagadas». Se imponen al condenado el pago de las costas ocasionadas por esta infracción penal, incluidas expresamente las de la acusación particular.

Contra la referida sentencia se interpuso recurso de apelación por la representación procesal de Eduardo, y una vez tramitado el mismo, se elevaron las actuaciones a la Audiencia Provincial de Madrid, Sección 30ª, que en el Rollo de Apelación nº 259/2022, dictó sentencia nº 123/2022, de 8 de marzo de 2022, cuyos hechos probados tienen el siguiente contenido:

— «Único: Se aceptan los relatados en la Sentencia apelada y se añade un último párrafo del siguiente tenor: «La sentencia se notifica a las partes el 28-4-20 y al Ministerio Fiscal el 17-2-21. El acusado solicita el 29-4-20 copia de la grabación de la vista oral para interponer recurso de apelación. Lo reitera el 2-7-20. No obtuvo respuesta hasta el 17-2-21, sin que ello sea achacable al acusado. El recurso de apelación se formula el 26-2-21 y no se admite a trámite hasta el 24-11-21».

Y cuyo fallo es del tenor literal siguiente:

«2020, por el Juzgado de lo Penal 3 de Móstoles, en Procedimiento Abreviado 220-2019, cuyo Fallo quedará redactado como sigue: "Que debo condenar y condeno a Eduardo como responsable en concepto de autor de un delito de descubrimiento y revelación de secretos empresariales del artículo 278.1 y 2 del Código Penal, concurriendo la atenuante simple de dilaciones indebidas, a la pena de tres años de prisión, inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de condena y multa de doce meses a razón de diez euros por día con responsabilidad personal subsidiaria para caso de impago de un día de privación de libertad por cada dos cuotas no pagadas. Se imponen al condenado el pago de las costas ocasionadas por esta infracción penal, incluidas expresamente las de la acusación particular."».

Una vez que las partes fueron notificadas de la sentencia, se procedió a preparar un recurso de casación. Este recurso se fundamentó en la infracción de la ley, así como en la violación de preceptos constitucionales y en el quebrantamiento de forma. Dicho recurso fue debidamente anunciado ante las autoridades competentes. Se remitieron a la Sala Segunda del Tribunal Supremo todas las certificaciones necesarias.

La representación del recurrente basó su recurso en los siguientes motivos:

1. «Por infracción de precepto Constitucional 24.2 CE. Se formula al amparo de lo dispuesto en el artículo 852 de la Ley de Enjuiciamiento Criminal y del artículo 5.4 de la Ley Orgánica del Poder Judicial, por vulneración del artículo 24.2 de la CE, y en concreto, por vulneración del derecho a utilizar los medios de prueba pertinentes para la defensa.
2. Por infracción de precepto Constitucional 24.1 CE. Se formula al amparo de lo dispuesto en el artículo 852 de la Ley de Enjuiciamiento Criminal y del artículo 5.4 de la Ley Orgánica del Poder Judicial, por vulneración del artículo 24.1 de la CE, y en concreto, por vulneración del derecho de defensa y por vulneración del derecho a no padecer indefensión.
3. Por infracción de Ley. Se formula al amparo de lo dispuesto en el artículo 849.1 de la LECRIM, por infracción de Ley, y en concreto, por indebida aplicación del artículo 278.1 y 2 del Código Penal, en relación con lo dispuesto en el artículo 142.2ª de la LECRIM y en el artículo 10 del Código Penal.
4. Por infracción de Ley. Se formula al amparo de lo dispuesto en el artículo 849.1 de la LECRIM, por infracción de Ley, y en concreto, por indebida aplicación del artículo 278.1 del Código Penal, en relación con el artículo 10 del Código Penal.
5. Por quebrantamiento de forma. Se formula al amparo de lo dispuesto en el artículo 851 de la LECRIM, en relación con el artículo 142.2ª de citada ley rituaria procesal ».

Instruidas las partes del recurso interpuesto, el Ministerio Fiscal y la parte recurrida, solicitan la inadmisión de todos los motivos, impugnándolos subsidiariamente; la Sala lo admitió, quedando conclusos los autos para el señalamiento de fallo cuando por turno correspondiera.

Una vez señalado el fallo, conforme a los procedimientos establecidos, se llevó a cabo la deliberación y votación el día 10 de julio de 2024. Durante esta sesión, los magistrados analizaron detalladamente los argumentos y pruebas presentadas por ambas partes. Tras una exhaustiva deliberación, se procedió a la votación, en la cual se decidió desestimar el recurso interpuesto.

Establece la propia Sentencia del Tribunal Supremo que en el hecho probado se recoge que Eduardo es mayor de edad, nacido en China con nacionalidad española y sin antecedentes penales. Que, en el año 2005, el acusado realizó trabajos como informático diseñando una página web para la empresa DIRECCION000, circunstancia que aprovechó para obtener, sin autorización, diversa información confidencial de la empresa DIRECCION001 relativa a su situación financiera, sus facturas y balances, y los listados de sus clientes. Que, en el mes de julio del año 2017, el acusado ofreció esta información comercial de la empresa DIRECCION001, en particular su listado de clientes, a otra empresa denominada 360 DH, SL, dedicada a la misma actividad comercial, llegándoles a mostrar el contenido de esta información y solicitando a cambio la cantidad de 1.500 €. Los responsables de la empresa 360 DH, SL sospecharon que el acusado pudiera haber obtenido esta información de forma ilícita, por lo que lo pusieron en conocimiento de la empresa DIRECCION001, cuyo propietario, Ismael, decidió denunciarlo. En la tarde del día 20 de julio de 2017, agentes del Cuerpo Nacional de Policía detuvieron al acusado cuando se encontraba en las inmediaciones de la empresa 360 DH, SL con la intención de hacer entrega de esta información comercial de la empresa DIRECCION001, la cual llevaba almacenada en un Pen Drive de la marca EMTEC que fue incautado por la policía en el momento de la detención. Previa autorización judicial acordada mediante auto de fecha 8 de septiembre de 2018 por el Juzgado de Instrucción nº 2 de Fuenlabrada, se procedió al examen de este dispositivo Pen Drive marca EMTEC, hallando almacenado en él una carpeta denominada «DIRECCION001» que tenía 5 carpetas en su interior con las siguientes denominaciones y contenido: Carpeta denominada «FACTURAS» con un fichero comprimido RAR que contenía diversos archivos de facturas de esa empresa y un archivo en formato PDF de otra factura. Carpeta denominada «JPG» que almacenaba un archivo de imagen llamado DIRECCION001 1 correspondiente a un pantallazo realizado a dos mensajes de correo electrónico DIRECCION002. Carpeta denominada «LISTA DE CLIENTES» que almacenaba

dos ficheros, uno de ellos en formato Excel que contenía el listado de los clientes de la empresa DIRECCION001 con nombre y apellidos, así como su teléfono y el email de contacto de su empresa. Carpeta denominada «RESUMEN VENTAS» que tenía almacenados diferentes archivos en los que obran el balance de la empresa DIRECCION001, ventas realizadas e información financiera de la misma. Carpeta denominada «SQL» que contenía dos ficheros denominados EQUIPAMIENTO COMERCIAL.

Considera el Tribunal Supremo, que del anterior relato fáctico -sin necesidad de su complemento con nuevos hechos que consten en la fundamentación jurídica- la concurrencia de los elementos del art. 278.1 y 2 debe ser mantenida, tal y como establecía la sentencia anterior

En efecto, tal como precisó la STS 864/2008, de 16-12: «El art. 278 sanciona un tipo de delito constituido por los elementos siguientes: La acción delictiva consiste alternativamente: En el apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos; o El empleo de algunos de los medios o instrumentos del apartado 1 del art. 197, el cual, a su vez, relaciona unos modos de comisión que aquí no interesa precisar».

Por lo que continúa estableciendo la sentencia que tal acción delictiva ha de tener por finalidad descubrir un secreto, esto es, «algo que conocen una o varias personas que tienen interés en que no lo conozcan los demás, particularmente los que se dedican a la misma clase de actividad ».

Ha de tratarse de un secreto de empresa, concepto más amplio que el de secreto industrial al que se refería el art. 499 de la anterior CP, ya que abarca no solo los relativos a la técnica de los procedimientos de producción, sino también los relativos al comercio u organización del negocio de que se trate.

Conviene decir aquí que nos encontramos con un delito que puede cometer cualquier persona, es decir, un delito común. No se trata de un delito especial propio que solo está al alcance de quienes reúnen determinadas características, como ocurre con el delito del art. 279 al que luego nos referiremos. Ha de

ser cometido por quien no conoce el secreto y trata de descubrirlo.

También considera el Tribunal Supremo en la sentencia objeto de análisis, que nos encontramos ante un delito de consumación anticipada. Basta la acción de apoderamiento dirigida a alcanzar ese descubrimiento. Conseguir el conocimiento del secreto pertenece a la fase posterior de agotamiento de la infracción. Incluso se comete, aunque no pueda después alcanzarse ese descubrimiento del secreto porque, por ejemplo, «el autor del delito no puede llegar a descubrir las claves utilizadas por la empresa en defensa de tal secreto».

Su difusión, revelación o cesión a terceros constituye la figura agravada del art. 278.2.

Por tanto, el elemento nuclear de este delito es el *secreto de empresa.* No define el Código Penal qué debemos entender por tal, seguramente por tratarse de un concepto lábil, dinámico, no constreñible en un «numerus clausus».

Por ello, el Tribunal considera que habremos de ir a una concepción funcional-práctica, debiendo considerar secretos de empresa «los propios de una actividad empresarial, que, de ser conocidos contra la voluntad de la empresa, pueden afectar a su capacidad competitiva. Así, serán notas características: la confidencialidad (pues se quiere mantener bajo reserva); la exclusividad (en cuanto propio de una empresa); el valor económico (ventaja o rentabilidad económica); licitud (la actividad ha de ser legal para su protección)». Su fundamento se encuentra en la lealtad que deben guardar quienes conozcan el secreto, por su relación legal o contractual con la empresa, ya que el bien específicamente tutelado consistirá en la competencia leal entre las empresas. Y su contenido suele entenderse integrado por los secretos de naturaleza técnico-industrial (objeto o giro de empresas); los de orden comercial (como clientela o marketing), y los organizativos (como las cuestiones laborales, de funcionamiento y planes de empresa). Su materialización puede producirse en todo género de soporte, tanto papel como electrónico y tanto en original como copia y aún por comunica-

ción verbal. Y cabe incluir tanto cifras, como listados, partidas contables, organigramas, planos, memorandums internos, etc.

También considera el Tribunal Supremo, al igual que resalta la doctrina más autorizada, que el art. 278.1 castiga a cualquier persona que se apropie de información, documentos, dispositivos o cualquier tipo de soporte que contenga un secreto empresarial, con la intención de revelarlo, está cometiendo un delito. Además, el uso de herramientas o métodos específicos para lograr este objetivo también está penalizado bajo esta normativa.

Este tipo de delito, conocido comúnmente como *espionaje industrial*, implica la obtención y uso indebido de información confidencial de una empresa. La finalidad de esta acción es generalmente obtener una ventaja competitiva o causar un perjuicio a la empresa afectada.

El bien jurídico protegido es la capacidad competitiva de la empresa. Este concepto se refiere a la habilidad de una empresa para competir de manera efectiva en el mercado, manteniendo su posición frente a otras empresas. La capacidad competitiva puede incluir diversos factores como la innovación, la eficiencia operativa, y la capacidad de atraer y retener clientes.

Algunos monografistas del tema, sin embargo, se muestran partidarios de la naturaleza pluriofensiva del delito. Estos expertos argumentan que el delito no solo afecta a un único aspecto, sino que tiene múltiples dimensiones. En este sentido, se protegería tanto el interés patrimonial del empresario titular del secreto, de carácter individual, como la preservación del sistema de competencia de mercado, de signo colectivo o socioeconómico. Esto significa que, además de proteger los intereses económicos del empresario que posee el secreto, también se busca mantener un sistema de competencia justo y equilibrado en el mercado.

La protección del interés patrimonial del empresario titular del secreto se centra en salvaguardar los activos y recursos que son vitales para la operación de la empresa. Estos activos pueden incluir información confidencial, estrategias comerciales, y otros recursos que proporcionan una ventaja competitiva. La

divulgación o el uso indebido de esta información puede tener consecuencias graves para la empresa, incluyendo pérdidas económicas y daños a su reputación.

Por otro lado, la preservación del sistema de competencia de mercado tiene un enfoque más amplio y colectivo. Este aspecto se refiere a la necesidad de mantener un entorno de mercado donde todas las empresas puedan competir en igualdad de condiciones. Un sistema de competencia saludable es esencial para la innovación, la eficiencia y el bienestar económico general. Las prácticas desleales o ilegales que distorsionan la competencia pueden perjudicar no solo a las empresas individuales, sino también a los consumidores y a la economía en su conjunto.

Continúa afirmando el Tribunal Supremo en esta sentencia que el «delito de descubrimiento de secretos es un delito de peligro concreto, ya que no se exige la causación de perjuicio efectivo alguno a la capacidad competitiva de la empresa. Es, además, un tipo mixto alternativo, resultando indiferente que se lleven a cabo una o varias de las acciones descritas ».

En palabras del Tribunal Supremo, «el secreto de empresa es toda información relativa a la industria o empresa que conocen un número reducido de personas y que, por su importancia (económica en este caso), el titular desea mantener oculta.

Dentro del secreto de empresa, se incluyen tanto las relativas a aspectos industriales como comerciales. Estos aspectos pueden abarcar desde los procesos de fabricación y producción, hasta las estrategias de marketing y ventas. El conocimiento de estos elementos puede afectar de manera significativa a la capacidad para competir en el mercado.

En la medida en que puedan también afectarle, se comprenden igualmente los datos sobre la situación financiera o fiscal de la empresa. Esto incluye información detallada sobre los ingresos, gastos, beneficios, deudas, y cualquier otra variable económica que pueda influir en la estabilidad y crecimiento de la empresa.

Solo podrán considerarse como tales las informaciones que realmente tengan la entidad suficiente para lesionar la capaci-

dad competitiva de la empresa. Es decir, deben ser datos que, si se divulgan, puedan causar un daño tangible y significativo a la posición de la empresa en el mercado. Esto excluye información trivial o de menor relevancia que no tendría un impacto considerable en la competitividad».

En cuanto al sujeto activo, recalca la sentencia que este puede ser cualquiera. Y establece que sujeto pasivo es el titular de la empresa, que puede ser distinto del propietario de los papeles o datos de los que se apodera el sujeto.

La conducta es doble. Puede consistir en apoderarse por cualquier medio de los soportes, cualquiera que sea su clase, en los que se encuentra el secreto, o en utilizar los medios del art. 197.1 CP, dirigidos a interceptar sus comunicaciones o utilizar artificios técnicos de escritura, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación.

Apoderarse es «tomar, coger, aprehender, cualquiera que sea la forma en que ello se haga y cualquiera que sea el soporte en el que se encuentre recogido el secreto: datos, documentos, escritos o electrónicas, soportes informáticos u otros objetos que se refieran al mismo». No hay delito si el sujeto no se apodera de nada, sino que simplemente aplica los conocimientos que por su cargo tenía.

Datos son las «unidades básicas de información, cualquiera que sea su contenido (un número, una palabra, un sonido, una imagen). Documento electrónico es todo conjunto de datos o de información creado informáticamente o susceptible de procesamiento informático. Soportes informáticos son los dispositivos físicos en donde se almacenan los ficheros o documentos electrónicos en los que se recoge el secreto de empresa, cualquiera que sea su naturaleza o funcionamiento (electromagnético, óptico, etc.)».

Se precisa el apoderamiento de los datos o soportes en los que se encuentra el secreto. Esto significa que, si el descubrimiento del mismo se hubiera producido por cualquier otro procedimiento, como de forma accidental, no será posible apreciar el delito. Por ejemplo, si alguien encuentra un documento con-

fidencial en la calle y lo lee sin intención de robarlo, no se considerará un delito. No obstante, esta cuestión es discutida. No faltan autores que defienden que basta con la captación intelectual del secreto, aunque no se coja materialmente nada. Es decir, leer el documento sin llevárselo físicamente.

Sin embargo, esta postura tiene una importante limitación. La simple captación mental del secreto será suficiente únicamente cuando la misma ha sido debida a alguna actuación del sujeto activo sobre el soporte. Esto implica que el individuo debe haber realizado alguna acción que le permita acceder al soporte, aunque sea por unos instantes. Por ejemplo, si alguien abre un cajón cerrado y lee un documento confidencial, aunque no se lo lleve, podría considerarse delito. La clave está en que el sujeto activo debe haber tenido la capacidad para acceder al conocimiento del secreto o información reservada que el mismo contiene.

En resumen, el debate se centra en si es necesario apoderarse físicamente del soporte del secreto o si basta con la captación intelectual del mismo. La interpretación más estricta requiere el apoderamiento material, mientras que la más laxa permite considerar delito la simple lectura del documento, siempre que haya habido una acción que permita acceder al soporte.

La segunda modalidad de conducta se refiere a los medios o instrumentos mencionados en el artículo 197.1. El primer inciso abarca el apoderamiento de cualquier tipo de dato, documento o soporte que se refiera al secreto de empresa, ya comentado previamente. En el segundo inciso se menciona la interceptación de las telecomunicaciones, que incluye todas las comunicaciones electrónicas que se producen a distancia mediante servicios disponibles para el público, tanto telefónicas (incluyendo la telefonía inalámbrica) como aquellas que empleen cualquier otro sistema de comunicación mediante señal, radio o videoconferencia.

Por interceptación se entiende la «captación del contenido de la comunicación, sin impedir que llegue a su destino. Esto incluye la conducta de copia, grabación o reproducción subrep-

ticia de datos, documentos o mensajes de correo electrónico que circulan por una intranet o por una red externa».

En el segundo inciso del artículo 197.1 se hace alusión a la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación. La rápida incorporación de las nuevas tecnologías al ámbito empresarial justifica la inclusión de una cláusula abierta, como la final, que permite dar cabida a las innovaciones. Por «artificio técnico» debe entenderse los medios técnicos idóneos para percibir, registrar o reproducir sonidos, imágenes o cualquier otra comunicación.

La finalidad de «descubrir un secreto de empresa», elemento subjetivo del injusto, debe ser la razón de la conducta. «Descubrir» es conocer algo que se ignoraba, aunque no se haga partícipe a otros de ello.

La consumación se produce, y así lo considera la propia sentencia, con el simple hecho del apoderamiento de los objetos o soportes en donde se contiene el secreto de empresa, o con la utilización de los medios técnicos, aunque el sujeto no llegue a conocer el contenido de los mismos.

Se trata de un delito de consumación anticipada en el que ésta se adelanta al momento en que se realiza la acción animada con el propósito requerido.

En cuanto al tipo agravado del artículo 278.2, que supone la revelación de secretos por quien los descubrió apropiándose de los soportes en donde se encuentran, la conducta es doble. Primero, el sujeto debe haber descubierto el secreto por los procedimientos del artículo 278.1. Después, debe transmitir esos secretos a otros. Por esta razón, se considera un tipo agravado del tipo básico mencionado en el apartado 1.

Este tipo agravado, el Tribunal Supremo lo clasifica como un tipo mixto alternativo, de peligro concreto. Esto se debe a que dar a conocer el secreto de empresa a terceros pone en riesgo la capacidad competitiva de la empresa. La acción castigada incluye difundir, revelar o ceder el secreto a terceros. «Difundir» se refiere a divulgar el secreto, sin importar el procedimiento utilizado para hacerlo. «Revelar» implica manifestar lo que antes

era desconocido. La «cesión a terceros» puede ser tanto onerosa como gratuita. La consumación del delito se alcanza cuando el secreto se pone en conocimiento de terceros, lo que constituye el resultado de la conducta.

El artículo 278.2 establece que la revelación de secretos es una conducta que no solo afecta a la empresa propietaria del secreto, sino que también puede tener repercusiones en el mercado y en la competencia. La protección de estos secretos es fundamental para mantener la integridad y la competitividad de las empresas. Por lo tanto, la ley castiga severamente la difusión, revelación o cesión de estos secretos a terceros.

En resumen, el tipo agravado del artículo 278.2 es una medida legal diseñada para proteger los secretos empresariales y garantizar que las empresas puedan operar en un entorno competitivo y justo. La revelación de secretos es una conducta grave que puede tener consecuencias significativas tanto para la empresa afectada como para el individuo que comete el delito.

La naturaleza del bien jurídico protegido hace que éste solo pueda considerarse lesionado cuando la revelación pueda afectar a la capacidad competitiva de la empresa. Esa aptitud va implícita en la difusión, que apunta al conocimiento general, y en la cesión, que sugiere también la transmisión a un tercero interesado.

Aunque es factible la tentativa, la doctrina considera, con razón, que debe incluirse en el tipo básico, sancionándose conforme al marco penal que en el mismo se establece. En efecto, como precisa la sentencia de instancia, sería paradójico, pues resultaría una pena superior para la tentativa del artículo 278.2 que para el delito consumado del artículo 278.1. Y es evidente que el artículo 278.1 ya castiga y prevé expresamente una pena para el tipo delictivo en grado inicial o de preparación, por lo que se debería estar al artículo 278.1 que expresamente está castigando una fase preparatoria.

En el caso que nos ocupa, claramente se infiere del hecho probado que el recurrente obtuvo sin autorización alguna diversa información confidencial de la empresa DIRECCION001 relativa a su situación financiera, facturas, listados de sus clien-

tes, balances, y que mostró esta información, contenida en un Pen Drive, a los responsables de otra empresa 360 HD SL, dedicada a la misma actividad, todo ello a cambio de 1.500 €.

La información confidencial obtenida por el recurrente incluía detalles críticos sobre la situación financiera de DIRECCION001, tales como ingresos, gastos, deudas y activos. Además, se accedió a facturas que reflejaban transacciones comerciales, así como listados de clientes que contenían datos personales y comerciales de los mismos. Los balances financieros proporcionaban un panorama completo de la salud económica de la empresa.

El recurrente, sin tener autorización para acceder a estos datos, los recopiló y almacenó en un Pen Drive. Posteriormente, se dirigió a los responsables de 360 HD SL, una empresa que opera en el mismo sector que DIRECCION001. Durante una reunión, el recurrente mostró la información confidencial a estos responsables, con el objetivo de obtener un beneficio económico. A cambio de esta información, recibió la suma de 1.500 €.

Este acto de obtención y divulgación de información confidencial sin autorización plantea serias cuestiones legales y éticas, ya que compromete la privacidad y la seguridad de los datos de DIRECCION001. Además, la acción de mostrar esta información a una empresa competidora podría haber tenido implicaciones significativas para la competitividad y el funcionamiento de DIRECCION001.

Se trata de una conducta que se integra en el artículo 278.1 y 2 CP en grado de consumación, dado que, como señalan las sentencias de instancia y apelación, la consumación se produce con la entrega del *Pen Drive* al encargado de la empresa 360 HD SL, sin que sea necesario que esta empresa descargue en sus sistemas la información, haga uso de la misma o llegue el *Pen Drive* a sus ordenadores. En efecto, el delito se consuma con la entrega, no solo por producirse en ese momento la cesión de los secretos a terceros, sino porque estamos, como ya se ha indicado, ante un delito tendencial que no requiere para su consumación que el tercero lo incorpore a su empresa, siendo suficiente la cesión o entrega de datos.

El motivo cuarto del recurso interpuesto por infracción de ley, al amparo de lo dispuesto en el artículo 849.1 LECrim, por aplicación indebida del artículo 278.1 CP, se desestima, ya que el recurrente no ha llevado a cabo acto de apoderamiento de información alguna, toda vez que el material del que disponía en su Pen Drive era información obtenida legítimamente por así habérsela facilitado tanto la empresa DIRECCION000 como su sucesora DIRECCION001.

Tal y como razona el Tribunal Supremo, el relato fáctico de la sentencia de instancia, aceptado en la apelación, se declaró probado que el recurrente tenía en su poder un Pen Drive que contenía diversa información confidencial de la empresa DIRECCION001, relativa a su situación financiera, sus facturas y balances y listados de sus clientes, que había obtenido aprovechando que realizó trabajos como informático, diseñando una página web para la empresa DIRECCION000, información que ofreció a un tercero, 360 HD SL, dedicada a la misma actividad comercial, a cambio de 1.500 €.

Igualmente se consideró acreditado que no contó con la autorización del titular de los datos para su obtención, apoderamiento y posterior revelación.

La analizada Sentencia 735/2024 del Tribunal Supremo confirma la importancia de la protección de los secretos empresariales en el ámbito del derecho penal. La sentencia destaca que la protección de los secretos empresariales es esencial para mantener la integridad y la confianza en las relaciones comerciales.

Por su parte, el fallo establece que la obtención ilícita de información confidencial, seguida de su ofrecimiento a terceros, constituye un claro ejemplo de violación de los derechos empresariales. Este tipo de conductas no solo vulneran la confidencialidad de la información de una empresa, sino que también pueden poner en peligro su posición competitiva en el mercado, justificando así la aplicación de sanciones penales severas. La sentencia enfatiza que la obtención y divulgación de secretos empresariales puede tener consecuencias devastadoras

para las empresas afectadas, incluyendo pérdidas financieras significativas y daños a su reputación.

Asimismo, la sentencia reafirma que la protección de los secretos empresariales no solo cubre los aspectos técnicos o industriales, sino también los datos comerciales, financieros y organizativos. El Tribunal ratifica que la revelación de este tipo de información, incluso si no llega a ser utilizada por terceros, es suficiente para considerar consumado el delito. La sentencia subraya que la protección de los secretos empresariales es amplia y abarca cualquier tipo de información que pueda ser considerada valiosa para la empresa y que no sea de dominio público.

Finalmente, la sentencia también refleja el compromiso del derecho penal con la protección de los activos empresariales como parte del sistema de competencia leal y resalta la necesidad de que las empresas adopten medidas de seguridad adecuadas para prevenir el acceso no autorizado a su información confidencial. La sentencia insta a las empresas a implementar políticas de seguridad rigurosas y a educar a sus empleados sobre la importancia de la confidencialidad y la protección de la información sensible.

En resumen, la Sentencia 735/2024 del Tribunal Supremo subraya la importancia de proteger los secretos empresariales y establece un precedente importante en el ámbito del derecho penal para garantizar la competencia leal y la integridad del mercado.

10. Dimensión del fenómeno delictivo

Impulsadas por el acelerado avance de la tecnología, las empresas de todos los sectores se encuentran inmersas en una carrera sin precedentes por la innovación. Este fenómeno no solo se limita a un ámbito específico, sino que abarca desde la industria tecnológica hasta el sector de servicios, afectando a pequeñas, medianas y grandes empresas por igual. Para destacar en un mercado cada vez más competitivo, no solo deben ser más inteligentes, rápidas y ágiles en su enfoque innovador, sino que también deben transformar la manera en que protegen sus innovaciones. En este contexto de alta velocidad, la atención que las empresas dedican a la protección de sus secretos empresariales puede marcar la diferencia entre el éxito y el fracaso, ya que la información confidencial puede ser un activo invaluable que, si se ve comprometido, puede llevar a la pérdida de ventaja competitiva.

Según el estudio «The Board ultimatum: Protect and Preserve. The Rising Importance of Safeguarding Trade Secrets 2017»[146] de Euromoney Institutional Investor Thought Leadership y Baker McKenzie, el 50% de los ejecutivos encuestados

146. Euromoney Institutional Investor Thought Leadership / Baker McKenzie. «The Board ultimatum : Protect and Preserve. The Rising Importance of Safeguarding Trade Secrets 2017». Recurso electrónico disponible en: https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets

afirmó que sus secretos empresariales son más valiosos que sus patentes y marcas registradas. Este dato resalta la percepción creciente de que la información estratégica y confidencial puede ser más crucial que los derechos de propiedad intelectual tradicionales. Aún más, el 69% anticipa que la protección de los secretos empresariales se volverá más crítica que la salvaguarda de otros tipos de derechos de propiedad intelectual, dado el rápido ritmo de la innovación tecnológica, lo que sugiere que las empresas deben adaptarse rápidamente a un entorno en constante cambio.

Un hallazgo clave de este estudio es que los secretos empresariales y la propiedad intelectual desempeñan un papel esencial en el valor de la marca de la empresa y en su estrategia corporativa. El 82% de los encuestados considera que los secretos empresariales son una parte importante, si no esencial, de sus operaciones. Este reconocimiento de su importancia se traduce en un enfoque más proactivo hacia la protección de esta información. Cerca de un tercio de los participantes lo clasificó como una de sus cinco principales preocupaciones, lo que indica que la gestión de estos secretos se ha convertido en una prioridad estratégica para muchas organizaciones.

A diferencia de otros tipos de propiedad intelectual, los secretos empresariales no requieren la presentación de solicitudes ante la Administración Pública. Esto significa que las empresas tienen la flexibilidad de proteger su información sin los largos y costosos procesos asociados con las patentes. Para protegerlos, todas las empresas deben implementar medidas que mantengan la confidencialidad de la información, lo que puede incluir desde acuerdos de no divulgación hasta la capacitación de empleados sobre la importancia de la seguridad de la información. Algunas compañías optan por resguardar parte de su propiedad intelectual como secreto empresarial precisamente para evitar la revelación de información confidencial durante el proceso de solicitud de patente, lo que puede ser un riesgo significativo.

Con la ola de innovación tecnológica y el aumento del uso de Internet, las empresas enfrentan un mayor riesgo de ser hackea-

das por competidores, gobiernos extranjeros y grupos hacktivistas. El espionaje empresarial patrocinado por Estados es una realidad creciente en una economía globalizada y cibernética, lo que obliga a las empresas a estar constantemente vigilantes y a invertir en medidas de seguridad cibernética. Lamentablemente, muchas empresas no comprenden el verdadero valor de su información confidencial hasta que esta es robada, lo que puede acarrear consecuencias devastadoras que van desde pérdidas financieras hasta daños irreparables a la reputación.

De acuerdo con diversos estudios demoscópicos[147], los empresarios consideran sus secretos empresariales de gran importancia para el crecimiento, la competitividad, la innovación y el desarrollo de sus negocios. Los sectores que realizan fuertes inversiones en I+D son los que otorgan mayor relevancia a los secretos empresariales, considerando su protección como un mecanismo más efectivo de recuperación de la inversión que las patentes u otros instrumentos de protección. Esto sugiere que la inversión en investigación y desarrollo no solo se trata de crear nuevos productos, sino también de proteger la información que hace posible esa innovación.

La Estrategia Española de Ciencia e Innovación 2013-2020 establece que «la investigación científica y técnica, el desarrollo y la innovación son factores indispensables para el crecimiento económico de un país y constituyen la base de su progreso y bienestar social».[148] Esta declaración subraya la importancia de fomentar un entorno donde la innovación pueda prosperar, lo que implica también la necesidad de proteger los secretos empresariales que son fundamentales para el éxito de esta investigación y desarrollo.

La reciente Ley 1/2019 de Secretos Empresariales resalta la importancia de estos secretos en su Preámbulo I, indicando que «las organizaciones valoran sus secretos empresariales tan-

147. ESTRADA I CUADRAS, A. El secreto empresarial. Una perspectiva jurídico-penal. Madrid, 2017, pág. 19.
148. Ministerio de Economía y Competitividad, pág. 8.

to como los derechos de propiedad industrial e intelectual y utilizan la confidencialidad como herramienta de gestión de la competitividad empresarial, de transferencia de conocimiento público-privada y de innovación en investigación. Sin embargo, las entidades innovadoras están cada vez más expuestas a prácticas desleales que buscan la apropiación indebida de secretos empresariales, como el robo, la copia no autorizada, el espionaje económico o el incumplimiento de los requisitos de confidencialidad. La globalización, la creciente externalización, las cadenas de suministro más largas y un mayor uso de tecnologías de la información y la comunicación contribuyen a aumentar el riesgo de tales prácticas. En consecuencia, la innovación y la creatividad se ven desincentivadas, disminuyendo la inversión, lo que repercute negativamente en el buen funcionamiento del mercado y merma su potencial como factor de crecimiento. Es necesario garantizar que la competitividad, sustentada en el saber hacer y en información empresarial no divulgada, esté adecuadamente protegida, mejorando las condiciones y el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos en el mercado. Una seguridad jurídica reforzada contribuiría a aumentar el valor de las innovaciones que las organizaciones buscan proteger como secretos empresariales, al reducir el riesgo de apropiación indebida», lo que pone de manifiesto la necesidad de un marco legal sólido que respalde la protección de estos activos.

Si se acepta que la maximización del nivel de vida de los ciudadanos es el principal objetivo económico del Estado y que la protección de los secretos empresariales estimula la investigación y el desarrollo, resulta lógico que el Estado tenga interés en proteger estos secretos de las empresas que ofrecen productos en sus mercados, cuando estos provienen de la inversión en I+D. Esto no solo beneficia a las empresas, sino que también tiene un impacto positivo en la economía en general, fomentando un entorno donde la innovación puede florecer y contribuir al bienestar social.

Entre los diversos tipos de ciberdelincuencia que han surgido en la era digital, el robo cibernético de información confidencial

empresarial se destaca notablemente como una de las actividades delictivas que ocasiona los mayores costos y pérdidas para las empresas. Esta actividad delictiva representa una de las principales amenazas para la estabilidad, la sostenibilidad y el crecimiento económico de las organizaciones que operan dentro de la Unión Europea, afectando no solo a las empresas individuales, sino también al panorama económico en su conjunto[149]

La información disponible sobre el robo cibernético de secretos empresariales es sorprendentemente limitada, tanto en términos cualitativos como cuantitativos. La evaluación de impacto realizada por la Comisión Europea en el año 2013, que se relaciona con la propuesta de la Directiva sobre la protección de conocimientos técnicos y la información comercial no divulgada, indica que «la recopilación de datos sobre el número total de casos de secretos comerciales en la Unión Europea es una tarea casi imposible». Además, los servicios de inteligencia de los Estados miembros admiten que operan «a tientas en la oscuridad» respecto a los casos de espionaje económico que se producen. Una de las principales razones que contribuyen a la falta de datos sobre el robo cibernético es que muchas intrusiones pasan desapercibidas, siendo detectadas en su mayoría de manera fortuita. Aun cuando se identifican, los incidentes rara vez son denunciados, ya que las empresas temen que admitir ser víctimas de apropiación indebida afecte negativamente su reputación y, en consecuencia, sus cotizaciones bursátiles[150].

---

149. Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018, pág. 22.

150. Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018, pág. 15. Recurso electrónico disponible en: https://publications.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en

Según el estudio titulado «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber»[151] publicado en diciembre de 2018, el robo cibernético de secretos empresariales se identifica como una de las amenazas más significativas para las empresas en la Unión Europea, tanto en términos de prevalencia como de impacto. Esta amenaza no solo se mantendrá en el tiempo, sino que se intensificará en el futuro a menos que se implementen acciones deliberadas y focalizadas por parte de organizaciones nacionales y supranacionales. El estudio también señala que, según el ECIPE, el robo cibernético ha causado pérdidas de alrededor de 60 billones de euros en crecimiento económico en la Unión Europea, lo que se traduce en una disminución de la competitividad y el empleo, así como en una reducción de las inversiones en investigación y desarrollo. En el año 2018, se estima que 289.000 puestos de trabajo estaban en riesgo, cifra que podría alcanzar un millón para el año 2025. Algunos sectores son más vulnerables que otros; por ejemplo, Verizon reportó 108 incidentes de espionaje cibernético en el sector manufacturero en el año 2016, siendo este el más afectado en la Unión Europea, con el 93% de los incidentes originados desde el exterior y el 91% relacionados con el robo o intentos de robo de secretos empresariales.

Los datos del estudio también revelan que el robo cibernético de secretos empresariales afecta más a las pequeñas y medianas empresas que a las grandes, debido a sus limitados presupuestos, la falta de conciencia sobre ser un objetivo de espionaje y la escasez de profesionales de TI cualificados. Es razonable suponer que el alcance real del problema puede ser significativamente mayor de lo que se estima actualmente, tan-

151. Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018, pág.

to en términos de número de incidentes como de impacto económico y social[152].

En Alemania, las pérdidas por violaciones de secretos empresariales alcanzaron la asombrosa cifra de 11.800 millones de euros anuales, con una de cada dos empresas alemanas siendo víctima de un caso de espionaje o intento de piratería industrial en los últimos dos años. Los sectores más afectados incluyen la automoción, aeroespacial, construcción de maquinaria, químico, farmacéutico y biotecnológico. En Estados Unidos, las pérdidas por violaciones de secretos empresariales se estiman entre 200 y 400 billones de dólares anuales. Un informe de 2017 indicó que el robo de propiedad industrial por parte de China costó a EE.UU. alrededor de 600 billones de dólares al año, lo que resalta la magnitud del problema a nivel internacional[153].

En este contexto, el Ministerio del Interior de Alemania ha criticado a las empresas alemanas por no implementar medidas de protección adecuadas para la información sensible desde una perspectiva competitiva frente a sus rivales extranjeros[154]. Asimismo, la Oficina Ejecutiva del Presidente de EE.UU. ha señalado que «las nuevas tendencias indican que el ritmo del espionaje económico y el robo de secretos comerciales contra las corporaciones estadounidenses se está acelerando». Los competidores extranjeros, algunos de los cuales están vinculados a gobiernos, han intensificado sus esfuerzos para robar información secreta empresarial mediante el reclutamiento de emplea-

---

152. Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018, pág. 57. Recurso electrónico disponible en: https://publications.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en

153. «El espionaje industrial acarreó pérdidas por 11.800 millones a la industria alemana». La Razón, 21 julio 2014. Recurso electrónico disponible en: https://www.larazon.es/internacional/el-espionaje-industrial-acarreo-perdidas-por-11-800-millones-a-la-industria-alemana-DM6961306

154. ESTRADA I CUADRAS, A. El secreto empresarial. Una perspectiva… Op., Cit., pág. 20.

dos actuales o ex-empleados. Además, se ha observado un aumento en la actividad de intrusión cibernética contra archivos electrónicos que contienen información de secretos empresariales, lo que amenaza no solo la seguridad económica de las empresas, sino también la seguridad nacional de EE.UU

Uno de los conflictos más relevantes en el ámbito de la tecnología y la seguridad a nivel global es el caso de Huawei, a la que EE.UU. acusa de espionaje industrial. Este problema abarca múltiples dimensiones, desde el uso de equipos extranjeros hasta la llegada de nuevas tecnologías como el 5G y la guerra comercial entre China y EE.UU. La controversia se remonta a 2003, cuando Huawei tuvo un grave conflicto con CISCO por infracción de patentes, lo que llevó a su retirada del mercado estadounidense. Un informe del Congreso de EE.UU. en 2012 identificó a Huawei y ZTE como amenazas potenciales para la seguridad nacional debido a su acceso a información confidencial. La desconfianza aumentó con la entrada en vigor de la Ley de Ciberseguridad china en 2017, que obliga a las empresas chinas a ceder información al gobierno cuando este lo requiera, lo que ha generado aún más preocupación en el ámbito internacional.

La batalla actual se intensificó a principios de 2018, cuando altos funcionarios de agencias de inteligencia de EE.UU. alertaron sobre los peligros del uso de dispositivos de Huawei y ZTE. El gobierno estadounidense ha llevado a Huawei a los tribunales, logrando la detención en Canadá de la vicepresidenta de la compañía, acusándola formalmente de robo de secretos empresariales, lo que ha añadido una capa adicional de tensión a las relaciones comerciales entre ambas naciones[155].

Ningún país en el mundo está exento de la posibilidad de sufrir espionaje empresarial, un fenómeno que ha cobrado relevancia en la actualidad. A medida que un país avanza y aumen-

155. «La CIA alerta de que Huawei ha sido financiado por el Estado chino». La Vanguardia. 20 abril 2019. Recurso electrónico disponible en: https://www.lavanguardia.com/internacional/20190420/461739362009/cia-alerta-huawei.html

ta su nivel tecnológico, también se incrementa el riesgo de que sus empresas se conviertan en blanco de ataques de este tipo, lo que puede tener consecuencias devastadoras para la economía y la seguridad nacional. En un caso notable ocurrido en 2015, la compañía holandesa ASML, reconocida como líder mundial en la provisión de sistemas de fotolitografía para la producción de circuitos integrados, comúnmente conocidos como chips, fue víctima de un acto de espionaje industrial. Este ataque fue llevado a cabo por varios empleados de origen chino que trabajaban en su Departamento de Investigación y Desarrollo ubicado en California. Estos individuos, actuando de manera clandestina, sustrajeron manuales secretos de instrucciones, software y lenguajes de programación, con el objetivo de compartir esta información valiosa con XTAL, una subsidiaria de otra empresa que mantiene vínculos indirectos con el gobierno chino. Tras la divulgación de un reportaje que reveló el espionaje industrial y el robo de tecnología que afectó a ASML, las acciones de la empresa experimentaron una notable caída en la bolsa, lo que refleja el impacto que tales incidentes pueden tener en la confianza del mercado.

En abril de 2019, los servicios secretos holandeses, conocidos por sus siglas AIVD en neerlandés, emitieron una alerta sobre los riesgos asociados con el uso de equipos fabricados en China en infraestructuras que son consideradas vitales por el gobierno. Esta advertencia incluyó la afirmación de que los ciberataques y el espionaje industrial provenientes de naciones como China, Rusia e Irán representan una «amenaza real» para la seguridad de las empresas y la integridad de la información sensible[156].

Las reservas y la cautela a la hora de entregar proyectos a empresas chinas, motivadas por el temor al espionaje, han permeado en gran medida en Europa. La Unión Europea se ha

156. FERRER, Isabel. «La holandesa ASML sufre el espionaje de un grupo de empleados chinos». El País, 20 abril 2019. Recurso electrónico disponible en: https://elpais.com/economia/2019/04/20/actualidad/1555760153_723256.html

convertido en el principal destino para las inversiones chinas, que en el año 2017 superaron los 35.000 millones de euros. De esta cifra, casi el 60% de este capital fue destinado a proyectos relacionados con infraestructuras y comunicaciones. Esta situación ha generado una creciente preocupación en varios países europeos respecto a la entrada de capital público chino en empresas que son consideradas estratégicas, ya que existe el temor de que tales adquisiciones puedan implicar una transferencia de tecnología hacia Pekín. Andrus Ansip, quien en ese momento ocupaba el cargo de vicepresidente de la Comisión Europea, denunció que China está exigiendo la implementación de puertas traseras (backdoors) obligatorias en los dispositivos, lo que consiste en secuencias que permiten eludir los sistemas de seguridad de un dispositivo, y que podrían ser utilizadas potencialmente para llevar a cabo actividades de espionaje industrial o estatal[157].

Un estudio realizado en 2014 por el Center for Strategic and International Studies reveló las dificultades inherentes a la evaluación del impacto financiero del espionaje empresarial. Sin embargo, se estima que el costo anual de la ciberdelincuencia para la economía mundial oscila entre 375 y 575 billones de dólares. Utilizando la estimación del Producto Interno Bruto (PIB) mundial de 74,9 trillones de dólares en 2013, proporcionada por el Banco Mundial, se puede inferir que la pérdida de secretos empresariales podría variar entre 749 billones de dólares y 2,2 trillones de dólares anuales, lo que representa una cifra alarmante que pone de manifiesto la magnitud del problema[158].

Se ha observado un notable aumento del 64% en los incidentes de seguridad atribuidos a empresas competidoras, algu-

---

157. PELLICER, Lluís. «Bruselas advierte de que la UE debe "tener miedo" de empresas chinas como Huawei». El País. 7 diciembre 2018. Recurso electrónico disponible en: https://elpais.com/internacional/2018/12/07/actualidad/1544186622_856998.html

158. Center for Strategic and International Studies. «Net Losses: Estimating the Global Cost of Cybercrime». Junio 2014.

nos de los cuales pueden contar con el respaldo de Estados. Este incremento puede deberse a que las compañías están descubriendo que la información se almacena cada vez más en formato digital, lo que facilita, abarata y acelera el robo de propiedad intelectual y secretos empresariales en comparación con el desarrollo de capacidades propias. En la ejecución de ataques, los competidores a menudo combinan sofisticadas técnicas de alta tecnología con métodos más tradicionales, como la contratación de empleados de la empresa objetivo, sobornos, extorsiones y promesas de nuevos empleos. Este aumento en los delitos cibernéticos atribuidos a Estados y competidores coincide con un incremento en el número de robos de propiedad intelectual y otra información sensible. En 2014, el robo de propiedad intelectual creció un 19% en comparación con el año anterior, lo que indica una tendencia preocupante[159].

De acuerdo con el estudio titulado «The Board Ultimatum: Protect and Preserve. The Rising Importance of Safeguarding Trade Secrets 2017», realizado por Euromoney Institutional Investor Thought Leadership y Baker McKenzie, se reveló que una de cada cinco empresas ha sido víctima del robo de secretos empresariales. El 20% de las empresas encuestadas admitieron haber sufrido este tipo de robo, mientras que un 11% adicional indicó que no estaban seguros si habían sido objeto de apropiación indebida, lo que sugiere que los incidentes de robo podrían ser aún más elevados de lo que se reporta oficialmente.

El Center for Responsible Enterprise and Trade (CREATe.org), en colaboración con PwC, estimó que el impacto del robo de secretos empresariales oscila entre el 1% y el 3% del PIB de una

159. PWC. «Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015». 30 de septiembre de 2014, pág. 11. Cálculos realizados por PWC en base a datos del Banco Mundial. Recurso electrónico disponible en: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

nación[160]. Por lo tanto, el potencial de pérdidas se torna aún más amenazador al considerar la probabilidad del riesgo en ciberseguridad, lo que subraya la necesidad urgente de implementar medidas de protección más efectivas para salvaguardar la información crítica y los secretos comerciales de las empresas.

La amenaza del ciberespionaje de secretos empresariales para la seguridad nacional ha sido reconocida por expertos en la materia, quienes advierten que la situación geopolítica actual fomenta un aumento en el ciberespionaje, dirigido tanto al sector público como al privado. Este fenómeno no solo proviene de actores estatales, sino también de organizaciones criminales que buscan obtener beneficios económicos a expensas de la seguridad de las empresas. La creciente sofisticación de las técnicas empleadas para acceder a secretos empresariales plantea un desafío significativo para la seguridad económica y la defensa nacional de los países afectados[161].

La Estrategia de Seguridad Nacional 2017 identifica el espionaje como una amenaza prioritaria, destacando que el espionaje industrial, cuyo objetivo es acceder a conocimientos tecnológicos y estratégicos, representa un desafío considerable que no puede ser ignorado. La colaboración entre el sector público y privado es esencial para abordar este fenómeno, dado el incremento de las agresiones provenientes de servicios de inteligencia extranjeros que buscan socavar la estabilidad económica de las naciones.

La necesidad de garantizar la ciberseguridad ha llevado a la implementación de diversas medidas en España y la Unión Europea, incluyendo la Estrategia Nacional de Ciberseguridad 2019, que establece acciones específicas contra el ciberespionaje para proteger el patrimonio tecnológico del país.

---

160. PWC. «Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015». 30 de septiembre de 2014, pág. 16.

161. CANDAU, Javier. «Ciberespionaje, una amenaza al desarrollo económico y la defensa». Seguritecnia. Enero 2019. Recurso electrónico disponible en: https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/3573-ciberespionaje-una-amenaza-al-desarrollo-economico-y-la-defensa/file.html

11. Conclusiones

A lo largo del presente trabajo se ha llevado a cabo un análisis exhaustivo y detallado del delito de revelación de secretos empresariales, un aspecto que resulta ser esencial para la protección del patrimonio inmaterial de las empresas en el contexto actual. Este estudio minucioso de la normativa vigente, que incluye especialmente el artículo 278 del Código Penal, así como la Ley 1/2019 de Secretos Empresariales, permite delinear un marco jurídico coherente y robusto que está destinado a salvaguardar los intereses económicos y competitivos de las empresas. Este marco se establece frente a las conductas ilícitas que implican la obtención, divulgación y uso indebido de información confidencial, que es vital para el funcionamiento de cualquier organización

El presente estudio sobre el delito de revelación de secretos en el ámbito empresarial ha permitido evidenciar la importancia fundamental de proteger los conocimientos adquiridos por las empresas en el curso de sus actividades comerciales y técnicas. La competencia leal y el correcto funcionamiento del mercado dependen de la capacidad de las empresas para salvaguardar sus secretos comerciales, lo que a su vez fomenta la innovación y el desarrollo tecnológico. Sin la protección adecuada, las empresas podrían verse vulnerables a prácticas desleales que comprometen su posición en el mercado y su capacidad para competir de manera justa.

En primer lugar, se ha comprobado que el bien jurídico protegido en estos delitos es la libertad de empresa, así como la capacidad competitiva de las organizaciones. La información confidencial o reservada constituye un activo de gran valor para las empresas, y su revelación o uso ilícito puede generar graves perjuicios económicos, no solo para la entidad afectada, sino también para la sociedad en su conjunto, al distorsionar el equilibrio de la oferta y demanda en el mercado. La pérdida de esta información puede resultar en una desventaja competitiva significativa, afectando la capacidad de la empresa para innovar y crecer.

Asimismo, se ha demostrado que el concepto de secreto empresarial debe ser comprendido de manera amplia, abarcando tanto los secretos industriales como los comerciales. Este enfoque holístico asegura que cualquier tipo de información relevante que confiera a la empresa una ventaja competitiva sea debidamente protegido por el ordenamiento jurídico. Además, las empresas deben adoptar medidas razonables para mantener la confidencialidad de dicha información, siendo estas medidas un criterio esencial en la aplicación de las disposiciones penales. Estas medidas pueden incluir la implementación de políticas de seguridad de la información, la capacitación de empleados y el uso de tecnologías de protección de datos.

La investigación ha dejado claro que la normativa española, tanto en el ámbito penal como en el mercantil, ha evolucionado significativamente en los últimos años para responder a los desafíos que plantea el acceso y uso indebido de los secretos empresariales en una era caracterizada por el rápido desarrollo tecnológico. La legislación vigente, junto con la jurisprudencia, ha establecido un marco robusto que no solo protege los intereses patrimoniales de las empresas, sino que también promueve un entorno de competencia justa, esencial para el progreso económico. Este marco legal incluye sanciones severas para aquellos que violen la confidencialidad de los secretos empresariales, disuadiendo así posibles infractores.

En conclusión, el delito de revelación de secretos en la empresa no solo afecta a los derechos individuales de los empre-

sarios, sino que también tiene implicaciones más amplias para la economía de mercado. Es necesario, por tanto, que el legislador continúe perfeccionando los mecanismos de protección de los secretos empresariales para garantizar que las empresas puedan operar en un entorno competitivo y justo, promoviendo así la innovación y el desarrollo económico. La protección efectiva de los secretos empresariales es crucial para mantener la confianza en el mercado y asegurar que las empresas puedan seguir invirtiendo en investigación y desarrollo sin temor a la apropiación indebida de su información valiosa.

El estudio también subraya la importancia de la cooperación internacional en la protección de secretos empresariales, dado que las empresas operan en un mercado globalizado. Las leyes nacionales deben estar alineadas con los estándares internacionales para asegurar una protección efectiva y uniforme. Además, la colaboración entre el sector público y privado es esencial para desarrollar estrategias efectivas de protección y respuesta ante la revelación de secretos.

Finalmente, se destaca la necesidad de una educación continua y la sensibilización de todos los actores involucrados, desde los empleados hasta los directivos, sobre la importancia de proteger la información confidencial. Solo a través de un esfuerzo conjunto y coordinado se podrá garantizar un entorno empresarial seguro y justo.

Realizar este trabajo ha supuesto para mí un proceso de gran aprendizaje y enriquecimiento. No solo he profundizado en un área específica del derecho penal que tiene gran relevancia en el contexto empresarial actual, sino que también he comprendido la importancia del equilibrio entre los derechos empresariales y la justicia penal. Este trabajo me ha permitido ver de cerca cómo las normativas jurídicas se aplican de manera concreta para proteger los intereses empresariales y fomentar un entorno competitivo saludable.

Durante el desarrollo de este estudio, he tenido la oportunidad de analizar casos prácticos y teóricos que ilustran cómo las leyes penales se implementan en situaciones reales. Esto me ha permitido entender mejor los desafíos que enfrentan las empre-

sas en términos de cumplimiento legal y las posibles consecuencias de no adherirse a las normativas establecidas. Además, he podido observar cómo la justicia penal no solo busca castigar, sino también prevenir conductas ilícitas que puedan afectar el mercado y la competencia.

Sin duda, el desarrollo de este estudio me ha ayudado a mejorar mis habilidades investigativas y me ha reafirmado en la importancia de la protección legal como base para el crecimiento económico y el bienestar social. He aprendido a valorar la meticulosidad en la investigación jurídica y la necesidad de estar siempre actualizado con las últimas reformas y cambios en la legislación. Este conocimiento no solo es valioso para mi desarrollo profesional, sino que también contribuye a mi entendimiento de cómo las leyes pueden ser una herramienta para el progreso y la estabilidad en el ámbito empresarial.

Bibliografía

Antón y Abajo, A. (2023). Criterios de delimitación del objeto del delito de revelación de secretos empresariales: skill and knowledge y secreto empresarial. *Diario La Ley*.

Bajo Fernández, M. (1978). *Derecho penal económico aplicado a la actividad empresarial.* Civitas.

Bajo Fernández, M. y. (2010). *Derecho penal económico.* Editorial Ramón Areces.

Barbero Santos, M. (1985). *Los delitos socio-económicos.* Universidad Complutense de Madrid.

Campuzano Laguillo, A., Palomar Olmedo, A., & Sanjuán y Muñoz, E. M. (2019). *La protección de secretos empresariales.* Tirant lo Blanch.

Carrasco Andrino, M. (1998). *La protección penal del secreto de empresa.* Cedecs.

Castro Moreno, A. (2006). El Derecho penal español ante el espionaje industrial y el secreto de empresa (artículos 278 a 280 CP). *Rivista Trimestrale di Diritto penale dell'Economia*.

Díez Repollés, J. (2007). *Los elementos subjetivos del delito. Bases metodológicas.* Marcial Pons.

Estrada i Cuadras, A. (2017). *El secreto empresarial. Una perspectiva jurídico-penal.* Marcial Pons.

Estrada i Cuadras, A. (2016). *Violaciones del secreto empresarial. Un estudio de los ílicitos mercantiles y penales.* Atelier.

Faraldo Cabana, P. (2009). *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico.* Tirant lo Blanch.

Farre Trepat, E. (2011). *Tentativa del delito: doctrina y jurisprudencia.* Edisofer.

Fernández Sánchez, M. (2000). *Protección penal del secreto de empresa.* Colex.

Fernández Seijo, J. (2020). *Ley de Secretos empresariales. Una aproximación práctica.* Aferré Editores.

Font Galán, J. (1987). *Constitución Económica y Derecho de la Competencia.* Tecnos.

Galán Corona, E. (2011). La Regulación contra la Competencia Desleal en la Ley de 10 de Enero de 1991. En A. Bercovitz Rodríguez-Cano, Galán Corona, E.; Quintana Carlo, I. y García-Cruces Gonzáles, J.A. *Comentarios a la ley de competencia desleal.* Aranzadi.

Gómez Segade, J. (1974). *El secreto industrial. Concepto y protección.* Tecnos.

González Cussac, J. (2013). *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación.* Tirant lo Blanch.

Gutiérrez Zarza, A. (2012). *Nuevas tecnologías, protección de datos y proceso penal.* La Ley.

Lissén Arbeloa, J. Y. (2019). Características, alcance de la protección conferida e implicaciones para las empresas en la nueva Ley de Secretos empresariales. *Diario La Ley.*

Luzón Pena, D. (2010). *Derecho penal de Estado social y democrático de Derecho.* La Ley.

Martínez-Buján Pérez, C. (2010). *Delitos relativos al secreto de empresa.* Tirant lo Blanch.

Molina Gimeno, F. (2009). Conveniencia político criminal de introducir la modalidad imprudente para complementar la protección penal de los secretos de empresa. *Diario La Ley.*

Morón Lerma, E. (2002). *La tutela penal del secreto de empresa, desde una teoría general del bien jurídico.* Departament de Ciència Política i de Dret Públic, Universitat Autònoma de Barcelona.

MUÑOZ CONDE, F. (2023). *Derecho Penal. Parte especial.* Tirant lo BLanch.

ORTS BERENGUER, E. Y. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática.* Tirant lo Blanch.

PRATS CANUT, J. (1997). Descubrimiento y revelación de secretos de empresa en el Código Penal de 1995. *Cuadernos de Derecho Judicial.*

PRATS CANUT, J.M. (1997) D*escubrimiento y revelación de secretos de empresa en el Código Penal de 1995. Delitos relativos a la propiedad industrial, al mercado y a los consumidores,* Madrid, Consejo General del Poder Judicial.

RODRÍGUEZ RAMOS, E., & RODRÍGUEZ RAMOS-LADARIA, G. Y. (2023). *Código Penal. Concordado y comentado con jurisprudencia.* La Ley.

SUÑOL LUCEA, A. (2009). *El secreto empresarial. Un estudio del artículo 13 de la Ley de Competencia Desleal.* Civitas.

Revistas y artículos de prensa

PWC. «Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015». 30 de septiembre de 2014.

Candau, J. «Ciberespionaje, una amenaza al desarrollo económico y la defensa». Seguritecnia. Enero 2019. Recurso electrónico disponible en: https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/3573-ciberespionaje-una-amenaza-al-desarrollo-economico-y-la-defensa/file.html

Center for Strategic and International Studies. «Net Losses: Estimating the Global Cost of Cybercrime». Junio 2014.

Ferrer, I. «La holandesa ASML sufre el espionaje de un grupo de empleados chinos». El País, 20 abril 2019. Recurso electrónico disponible en: https://elpais.com/economia/2019/04/20/actualidad/1555760153_723256.html

Pellicer, L. «Bruselas advierte de que la UE debe «tener miedo» de empresas chinas como Huawei». El País. 7 diciembre 2018. Recurso electrónico disponible en: https://elpais.com/internacional/2018/12/07/actualidad/1544186622_856998.htm

—«La CIA alerta de que Huawei ha sido financiado por el Estado chino». La Vanguardia. 20 abril 2019. Recurso electrónico disponible en: https://www.lavanguardia.com/internacional/20190420/461739362009/cia-alerta-huawei.html

Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018. Recurso electrónico disponible en: https://publications.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en

—«El espionaje industrial acarreó pérdidas por 11.800 millones a la industria alemana». La Razón, 21 julio 2014. Recurso electrónico disponible en: https://www.larazon.es/internacional/el-espionaje-industrial-acarreo-perdidas-por-11-800-millones-a-la-industria-alemana-DM6961306

Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018. Recurso electrónico disponible en: https://publications.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en

Comisión Europea / PricewaterhouseCoopers. «The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber». Diciembre 2018.

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD. «Estrategia Española de Ciencia, Tecnología e innovación 2013-2020». Recurso electrónico disponible en: https://www.ciencia.gob.es/dam/jcr:49a4ab93-ce39-4034-bdaf-e3bf999cb51f/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf

Publications Office of the European Union. (2013, 28 noviembre). 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, /* COM/2013/0813 final - 2013/0402 (COD) */, CELEX1. Publications Office Of The EU. Recurso electrónico disponible en: https://op.europa.eu/en/publication-detail/-/publication/0e7bac3f-5c28-11e3-914b-01aa75ed71a1/language-es

SENTENCIAS Y JURISPRUDENCIA

TRIBUNAL CONSTITUCIONAL. Sentencia del Tribunal Constitucional 88/1986, de 1 de julio. (BOE núm. 174, de 22 de julio de 1986). ECLI:ES:TC:1986:88

TRIBUNAL SUPREMO. STS 4811/1964, de 14 de noviembre. ECLI:ES:TS:1964:3123.

TRIBUNAL SUPREMO. STS de 4 de abril de 1972

TRIBUNAL SUPREMO. STS 772/2004, de 16 de junio de 2004

TRIBUNAL SUPREMO. STS 1169/2006, de 24 de noviembre de 2006

TRIBUNAL SUPREMO. STS 126/2007, de 5 de febrero.

TRIBUNAL SUPREMO. STS 285/2008, 12 de mayo de 2008. Roj: STS 2885/2008.

TRIBUNAL SUPREMO. STS 359/2008 de 19 de junio.

TRIBUNAL SUPREMO. STS 864/2008, 16 de diciembre de 2008. Roj: STS 7442/2008

TRIBUNAL SUPREMO. STS 129/2011, de 10 de marzo.

TRIBUNAL SUPREMO. STS 623/2015, de 13 de octubre de 2015

TRIBUNAL SUPREMO. STS 679/ 2018, de 20 de diciembre. Roj: STS 4422/2018

TRIBUNAL SUPREMO. STS 1379/2021, de 15 de abril de 2021

TRIBUNAL SUPREMO.STS 363/2023, de 17 de mayo de 2023

TRIBUNAL SUPREMO. STS 1442/2023, de 20 de octubre

TRIBUNAL SUPREMO. STS 444/2024, de 3 de abril.

TRIBUNAL SUPREMO. STS 735/2024 de 12 de julio de 2024.

AUDIENCIA PROVINCIAL DE CASTELLÓN. SAP Castellón, 28 de febrero de 2022 - Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039ª

AUDIENCIA PROVINCIAL VIZCAYA. SAP Vizcaya (Sección 6ª), 235/2005, de 26 de abril. ES:APBI:2005:1153.

SAP Barcelona 178/2011, 28 de febrero de 2011. Roj: SAP B 1349/2011 - ECLI:ES:APB:2011:1349.

SAP Córdoba 48/2007, 12 de marzo de 2007. Roj: SAP CO 689/2007 - ECLI:ES:APCO:2007:689.

AAP Castellón, a 28 de febrero de 2022. Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039ª

SAP Valencia, a 16 de septiembre de 2022. Roj: SAP V 2961/2022 - ECLI:ES:APV:2022:2961.

AAP Castellón, a 28 de febrero de 2022. Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039A.

AAP Castellón 118/2022, de 28 de febrero de 2022. Roj: AAP CS 2039/2022 - ECLI:ES:APCS:2022:2039ª

AUDIENCIA PROVINCIAL DE CASTELLÓN. SAP Castellón 118/2022, de 28 de febrero de 2022.

El texto analiza la creciente necesidad de proteger los secretos empresariales frente a las amenazas que plantea el desarrollo tecnológico, el cual facilita nuevos métodos de captación de información. Se argumenta que la información y el conocimiento adquirido por una empresa (su «patrimonio inmaterial») son un activo valioso, susceptible de ser explotado económicamente, y que atrae a competidores que buscan obtener ventajas sin el esfuerzo económico o laboral correspondiente.

El ordenamiento jurídico debe, por tanto, proteger la libre competencia y el derecho de las empresas a progresar según sus propios méritos. La vía más efectiva, según el texto, es la tipificación penal. El análisis se centra en el delito de revelación de secretos de empresa, regulado en los artículos 278 a 280 del Código Penal español. Esta protección va más allá de la mera indemnización civil, ya que la sustracción de secretos no solo perjudica económicamente a la empresa víctima, sino que también altera el sistema de oferta y demanda, afectando al mercado en su conjunto.

El estudio se propone definir el concepto clave de «secreto empresarial» (información que otorga una ventaja competitiva) y diferenciarlo de los delitos contra la intimidad personal (Art. 197). Se detallan las tres modalidades delictivas principales: el espionaje industrial o apoderamiento ilegítimo (Art. 278), la vulneración del deber de guardar secreto por parte de quien tiene acceso legítimo —como un empleado— (Art. 279), y el uso de un secreto sabiendo que su origen es ilícito (Art. 280).

Finalmente, el estudio justifica la intervención del Estado en esta materia. Si las empresas no gozan de protección legal, se ven obligadas a invertir costosos recursos en autoprotección, restando capital a la inversión en I+D e innovación. Esto frena el crecimiento económico y el bienestar social, una preocupación compartida a nivel europeo. El análisis propuesto utilizará legislación, doctrina y la jurisprudencia del Tribunal Supremo para delimitar el alcance de estos delitos.

Atelier
LIBROS JURÍDICOS

ISBN 979-13-87867-94-2
9 791387 867942