

CAPÍTULO TERCERO

LAS ACCIONES TÍPICAS COMO MODALIDADES ATENTATORIAS DEL BIEN JURÍDICO

I. Consideraciones preliminares.

Una vez concluido el análisis pormenorizado del objeto, conviene ahondar ya en el segundo de los aspectos que, desde la especial incidencia que en él asume el bien jurídico, contribuirá a definir el ámbito de lo punible, a saber, las acciones típicas o los medios comisivos.

En coherencia al entendimiento del secreto empresarial como estratégico acto competitivo, en la interpretación de las acciones ha devenido indispensable acudir, también, al derecho de la competencia desleal, puesto que, en esta disciplina se obtienen los criterios que proyectados a los medios comisivos determinan cuándo éstos se convierten en punibles. Según se sabe, en estos delitos, no se trata de garantizar o

evitar un determinado resultado, sino que se persigue castigar el ***modo ilícito*** de acceder, revelar o utilizar la información empresarial reservada.

Esta inteligencia del modo de agresión al interés tutelado condiciona la interpretación de los tipos. De ahí que el modelo exegético por el que se ha optado se proyecta sobre la estructura esencial adoptada por el código, pero no a partir del análisis de los preceptos, sino de las propias acciones típicas. Ello resulta congruente con la trascendencia que asumen las formas de afectación del bien jurídico en estos delitos.

En esta medida, el análisis de los diversos modos de ataque a la información reclama, en primer lugar, una interpretación exhaustiva del concepto o contenido de las modalidades atentatorias en relación al bien jurídico protegido y al objeto material del delito. A partir de esa significación, podrá ya detectarse qué conductas se hallan expresamente contempladas en el código y, acometer, en consecuencia, un análisis crítico de las mismas, así como identificar qué tipo de ataques se hallan ayunos de referencia legal.

En esta demarcación del ámbito de lo punible, únicamente se hace referencia a aquellos aspectos, que, en función de la metodología adoptada, resultan especialmente indispensables. Así, en algunas de las modalidades de acción típica (acceso y utilización), cobra una relevancia especial el ánimo con el que son acometidas, lo que explica que sea necesario abordar, particularizadamente, el elemento subjetivo del injusto, a partir de cuya presencia queda trazada la propia parte objetiva del tipo. En cuanto al resto de aspectos que podrían plantearse, sólo se destacarán aquellos en los que, desde la afección al bien jurídico protegido y en relación a las diversas

modalidades de acción típica, presentan mayor particularidad y que, dependiendo de la modalidad de que se trate, residirá en la estructura típica que le corresponde, en el *iter criminis*, entre otras cuestiones.

El orden metodológico que se seguirá en el examen de las modalidades atentatorias de los secretos viene proporcionado por la propia naturaleza de estos delitos. Así, se analizarán, en cuanto modalidades de acción típica, el acceso, la difusión, revelación y cesión y la utilización, que se hallan expresamente previstas en el código, junto con otras conductas atentatorias ilícitas, que se hallan desprovistas de referencia legal expresa o autónoma, pero que asumen una entidad lesiva análoga.

II. Acceso ilícito.

1. «Apoderamiento».

1.1. Concepto de «apoderamiento».

El apoderamiento constituye la primera de las modalidades típicas de acceso ilícito. Esta acción se corresponde con la conducta nuclear prevista en el artículo 278.1 CP, que, revistiendo una estructura mixta alternativa, exige que el sujeto activo, para descubrir un secreto de empresa: a) «se **apoderare** por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo» o b) «empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197».

Cualquiera de las modalidades atentatorias perpetrables en este ámbito debe ser interpretada desde la atención a la peculiaridad del objeto

material del delito --secreto de empresa-- sobre el que recae la acción. Según se sabe, el secreto empresarial consta de un elemento inmaterial o intelectual (***corpus mysticum***) y de un elemento material o corpóreo (***corpus mechanicum o extrinsecum***)¹²⁵³. El elemento inmaterial está constituido por una información propia del ámbito empresarial en los términos descritos. El elemento corporal puede consistir en escritos, soportes informáticos, fotografías, planos, proyectos, modelos, maquinaria, etc., idóneos como sostén de la información que en cada caso se trate. El auténtico secreto empresarial está integrado por el primer elemento; el segundo deviene mero soporte material del elemento inmaterial al que nada añade, puesto que no aporta a la información ningún valor intrínseco adicional. Estos elementos materiales sólo ostentan valor accesorio, a modo de signos externos que permiten reconocer la existencia del secreto y cuya disposición proporciona enormes ventajas para la aprehensión de la información en el quehacer diario de la actividad económica. Así pues, no debe confundirse la estructuración del secreto en los citados elementos con la pretendida distinción entre objeto material e inmaterial del secreto, que encierra una grave confusión¹²⁵⁴. El ***objeto del secreto siempre es inmaterial***, aunque se incorpore a un elemento material que lo haga perceptible. Y sobre este último elemento material, que exterioriza el secreto, generalmente, recae la acción típica.

Así pues, desde esta cualidad de ***intangibilidad*** o ***inmaterialidad*** intrínseca al secreto de empresa deberá interpretarse el objeto ***material*** del delito¹²⁵⁵. Desde luego, ello insinúa ya la dificultad e incomodidad que, en

¹²⁵³ Así, vid. supra capítulo I, de esta segunda parte del trabajo, destinado al análisis del objeto.

¹²⁵⁴ Vid. GÓMEZ SEGADE, J.A., "En torno al concepto...", en ***op. cit.***, pp. 420-421.

¹²⁵⁵ En este trabajo, se hace referencia al objeto material del delito para diferenciarlo del objeto jurídico o formal, que alude al bien jurídico o interés tutelado (así, vid. MIR PUIG, S., ***Derecho penal, Parte general, op. cit.***, p. 199). Sin embargo, no se distinguirá –puesto que,

estos delitos, se suscita ante el empleo de categorías o fórmulas tradicionales, acuñadas para conductas y delitos de corte clásico y, en esa medida, con una configuración esencialmente distinta a los analizados en esta investigación. En cualquier caso, desde esta específica *incorporeidad* que caracteriza al secreto de empresa, como objeto material del delito y de la acción, debe procederse a la exégesis del verbo nuclear de esta primera modalidad.

El término «apoderarse» debe ser interpretado como la aprehensión, obtención o adquisición de la información constitutiva del secreto de empresa. En este ámbito, pues, el apoderamiento no puede ser dotado de sentido desde un entendimiento clásico del mismo, formulado en los delitos contra el patrimonio y, por tanto, interpretado como un apoderamiento material, con desplazamiento físico de cosa aprehensible¹²⁵⁶. Ello supondría una interpretación sesgada y restrictiva de la acción típica desatenta a las características del objeto del delito.

en este ámbito, no parece asumir una relevancia que así lo aconseje-- entre el **objeto material del delito**, como «concreta realidad empírica a la que se refiere la acción típica» (así, vid. MIR PUIG, S., “Ojeto del delito”, en *Nueva Enciclopedia Jurídica*, XVII, p. 765) [en nuestro caso, el elemento material o corpóreo en el que se exterioriza el secreto --**corpus mechanicum**--] y el **objeto de la acción**, como concepto que no necesariamente demanda una realidad material [en este ámbito, el elemento inmaterial o intelectual que integra el secreto -- **corpus mysticum**--, esto es, la información]. Como se ha expuesto, generalmente, la acción típica recaerá sobre el elemento material, de modo que, en la mayor parte de casos, coincidirán objeto de la acción y objeto material. De ahí que, aunque conceptualmente sean desgajables, no se ha considerado necesario dilucidar qué modalidades típicas reclaman ineludiblemente la materialización del objeto del secreto de empresa y, por tanto, requieren, asimismo, objeto material del delito y qué modalidades no lo hacen (vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, pp. 236-237, para tal distinción en las modalidades típicas del art. 279 CP). En suma, pues, el objeto material del delito designa el secreto de empresa y, por tanto, alude, indistintamente, a la información que compone su objeto y a los elementos que lo hacen perceptible.

¹²⁵⁶ Así, vid. MORALES PRATS, F/MORÓN LERMA, E., en AA VV (QUINTERO OLIVARES, Dir.), *Comentarios al Nuevo Código Penal*, Pamplona, 2ª ed., 2001, p. 1281; MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, *op. cit.*, p. 73; GUTIÉRREZ FRANCÉS, M.L., “Notas sobre la delincuencia informática...”, en ARROYO ZAPATERO, L./TIEDEMANN, K., *Estudios de derecho...*, *op. cit.*, p. 196; SUÁREZ GONZÁLEZ, C., en AA VV, (RODRÍGUEZ MOURULLO, G., Dir.), *Comentarios al Código Penal*, Madrid, 1997, p. 803.

Así, el tipo comprende conductas de captación mental o intelectual¹²⁵⁷, sin desplazamiento físico (apoderamiento de datos) y conductas de apoderamiento físico subrepticio de los objetos que incorporan el secreto (apoderamiento de documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo). En suma, pues, el verbo 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. Esto es, advertida la especificidad del objeto –su inmaterialidad–, resulta accesorio el soporte que la contenga¹²⁵⁸.

La aproximación al bien jurídico protegido desde el derecho de la competencia desleal conduce, en este punto, al reconocimiento del carácter no reprochable de las acciones en sí mismas, de modo que el apoderamiento reclamará conceptualmente una adquisición o aseguramiento de la información acometida **de forma indebida**. Es decir, el apoderamiento de secretos no es una modalidad concurrencialmente reprochable en sí misma,

¹²⁵⁷ En contra, vid. GUTIÉRREZ FRANCÉS, M.L., “Delincuencia económica e informática en el nuevo Código Penal”, en *Ámbito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, CGPJ, Madrid, 1996, p. 288.

¹²⁵⁸ Esta accesoriedad debe ser entendida como una cuestión irrelevante a los efectos de considerar la adquisición de información, con independencia del soporte que la contenga, **apoderamiento ilícito**. Ahora bien, actualmente, la distinta naturaleza que puede revestir el soporte de la información determina peculiaridades y diferencias que deben ser advertidas y trasladadas a la configuración técnica de su tutela. Como se analizará posteriormente (vid. infra epígrafes relativos a las siguientes modalidades comisivas), hoy en día la mayor parte de la información empresarial reservada se almacena en redes, soportes o sistemas informáticos, desde los que se procesa y se transmite. El moderno sistema de almacenaje y transmisión de la información ha suscitado la aparición de modalidades de ataque especialmente insidiosas. Estos nuevos focos de peligro sobre la información contenida en soporte digital hará indispensable garantizar su seguridad y para ello deberá analizarse cuáles son las características de esa información que deben ser preservadas. Al respecto, para evaluar rápidamente el enjambre de nuevas cuestiones que conlleva la implantación de las nuevas tecnologías, basta pensar en lo fácil que resulta borrar datos de un secreto empresarial contenido en un disquete, a diferencia de lo que ocurre si se trata de llevar a cabo la conducta de destrucción sobre un secreto, que, por el contrario, se halla exteriorizado en un documento o soporte analógico.

sino por las circunstancias **ilícitas** en que tiene lugar (entre otras, las atinentes al elemento subjetivo¹²⁵⁹).

Estrechamente vinculado a lo anterior debe interpretarse la cláusula de cierre que incorpora la conducta tipificada en el art. 278.1 CP («El que, para descubrir un secreto de empresa, se apoderare **por cualquier medio...**»). En este caso, la acción típica se integrará únicamente por las conductas de apoderamiento ilícito, que, como advierte MARTÍNEZ-BUJÁN¹²⁶⁰, incorporan un específico desvalor de acción y, a nuestro juicio, también un específico desvalor de resultado. Así pues, la órbita típica se ceñirá a los supuestos de obtención de la información de modo ilícito, que, en el supuesto que nos ocupa, supondrá una obtención con apropiación indebida del esfuerzo ajeno y sin actividad propia.

De ahí que la amplitud que dicha cláusula --por cualquier medio-- introduce resulte sólo aparente puesto que sufre una notable restricción a través de un doble diafragma. De una parte, el ámbito de la infracción penal se limita a los **apoderamientos ilícitos sin actividad propia y con apropiación del esfuerzo ajeno, que suelen acometerse empleando medios comisivos especialmente reprobables y/o insidiosos (apoderamientos subrepticios de los soportes, captación intelectual de la información --lectura o escucha--, acceso a los datos)**¹²⁶¹. De otro lado, la presencia de elementos subjetivos del injusto desempeña asimismo una **función restrictiva** y selectiva de las conductas típicas.

¹²⁵⁹ Vid. infra, epígrafe destinado al elemento subjetivo como criterio delimitador del ámbito típico.

¹²⁶⁰ MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 72.

¹²⁶¹ Análogamente, MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, pp. 72-73 y, como advierte este autor, así fue propuesto ya por GUINARTE CABADA, G., "Consideraciones político-criminales...", en *EPCr., op. cit.*, p. 172.

En suma, pues, dicha expresión («...**por cualquier medio...**») debe ser entendida como una **cláusula de equiparación valorativa con el resto de medios comisivos a los que remite el precepto**¹²⁶². Y, en esa medida, el **ámbito típico** del art. 278.1, primer párrafo CP, que la incorpora, sanciona el apoderamiento del secreto empresarial **por cualquier medio abusivo, ilícito, indebido**.

Así, aunque lo relevante en esta modalidad descansa en ese **apoderamiento indebido** y en que la conducta se proyecte sobre el secreto de empresa, el código penal en vez de concebir esta previsión de forma genérica, ha preferido, de modo acertado, para evitar posibles lagunas, identificar concretamente el sustrato material en el que puede recaer la acción de apoderamiento. Parece indudable que, dependiendo de la corporeidad con la que se vertebra el secreto de empresa, la naturaleza de la conducta delictiva podrá variar, aunque no sustancialmente, en algunos aspectos y, por tanto, plantear alguna particularidad.

Los diversos objetos de referencia a los que se vincula o sobre los que puede recaer la acción típica en el código penal consisten en datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al secreto. De ahí la conveniencia de examinar brevemente la interpretación del ámbito específico que cada uno de ellos puede asumir.

I) Por lo que se refiere al elemento típico cifrado en los **«datos»**, se trata de una importante novedad introducida por el código vigente y que supone un notable avance respecto de la regulación prevista en anteriores

¹²⁶² En sentido análogo, vid. CARRASCO ANDRINO, M.M. “La tutela penal del secreto comercial y la concreción de la obligación de reserva: un análisis de la reciente jurisprudencia”, en **Revista de Derecho Penal y Criminología**, nº 7, 2000, p. 391.

tareas prelegislativas que no lo contemplaban (ni el artículo 276.1 PANCP 1983 ni el art. 284.1 PCP 1992 hacían referencia a este elemento). Por «datos» debe entenderse la propia información, conocimientos o ideas atinentes a cualquier ámbito de la actividad empresarial, que constituyen objeto del secreto de empresa. Parece que, con el término «datos», que no son objetos, el legislador intenta destacar ese elemento incorpóreo e intangible en que se cifra el secreto y dar cabida, así, a la modalidad de aprehensión inmaterial sin necesidad de apoderamiento de ningún soporte material.

Así, el apoderamiento de datos englobará esencialmente acciones de este tenor, es decir, captaciones intelectuales o mentales¹²⁶³, por ejemplo, por mera escucha o lectura física, por memorización o, como sugieren, MORENO CÁNOVAS y RUIZ MARCO¹²⁶⁴, al anotar de puño y letra en un bloc de propiedad las proporciones exactas en las que deben mezclarse dos componentes químicos para obtener un efecto analgésico. En esta medida, la captación intelectual del secreto se producirá con independencia del soporte en el que se encuentre exteriorizado el secreto. En el caso de aprehensión por lectura física, será pues irrelevante la naturaleza analógica o digital del soporte en el que se halle registrado el secreto, pues lo relevante radica en la **captación inmaterial** de los datos o de la información. Así, esta primera modalidad analizada (apoderamiento de datos) se proyectará de igual modo en el caso de que un sujeto lea en un documento de papel el listado de proveedores de tejidos de una empresa de diseño de ropa, como si el sujeto lee en pantalla de un ordenador la misma información digitalizada y registrada en un soporte informático.

¹²⁶³ En sentido contrario se manifiestan BAJO FERNÁNDEZ, M./BACIGALUPO, S., *op. cit.*, p. 495.

¹²⁶⁴ MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos*, Zaragoza, 1996, p. 126.

Por el contrario, mayor complejidad reviste el supuesto en que no sólo se produce el apoderamiento de un documento contenido en cualquiera de las memorias electrónicas del ordenador, sino también la posterior **reproducción ilícita del mismo en un disquete por el sujeto a fin de procurarse certeramente el contenido de la información**. Desde luego, en principio, en cuanto a la posible subsunción de esta conducta en el vigente código, para elucidar si quedará incluida en alguna de las modalidades de acceso ilícito, ya sea en la primera modalidad de apoderamiento (prevista en el art. 278.1, primer párrafo CP) o en la siguiente de interceptación (contemplada en el art. 278.1, segundo párrafo y 197.1, segundo párrafo CP) o, por el contrario, en ninguna de ellas, deberán ponderarse diversos criterios como la insidiosidad del medio empleado o el carácter más o menos restrictivo que se otorgue al ámbito típico de estas modalidades en virtud de una interpretación del precepto teleológicamente orientada. En cualquier caso, se estima oportuno avanzar en el estudio de estas modalidades y, posteriormente, acudir de nuevo a su análisis, como específico ámbito de especial problemática¹²⁶⁵. Así, pues, aun aplazado hasta ese momento, valga anticipar que el problema se planteará únicamente 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. En este último caso, cuando la reproducción sea telemáticamente la conducta quedará subsumida en la modalidad típica relativa a la interceptación o control ilícito de señales de comunicación¹²⁶⁶.

¹²⁶⁵ La conducta de reproducción constituye una modalidad atentatoria equiparable al acceso ilícito, que, sin embargo, no se halla específicamente prevista. Así, vid. infra, epígrafe relativo a otras conductas ilícitas asimiladas al acceso ilícito.

¹²⁶⁶ En sentido contrario, vid. FERNÁNDEZ SÁNCHEZ, M.T., *Protección penal...*, op. cit., pp. 232-233, que subsume esta conducta en la primera modalidad del precepto, relativa al apoderamiento y además la limita a la copia de informaciones que se encuentren en el disco duro del ordenador. Téngase en cuenta que el ordenador, al margen de la memoria ROM

II) La interpretación del elemento relativo a los «**documentos electrónicos**» debe acometerse desde la inteligencia de la remisión que el precepto efectúa a la modalidad típica del artículo 197.1 CP, cuyo análisis se llevará a cabo en la siguiente acción objeto de estudio. Así, a fin de otorgar un ámbito propio a cada modalidad típica, el apoderamiento de estos documentos debe limitarse a la **aprehensión material** de los objetos que incorporan el secreto. Esto es, el apoderamiento de documentos electrónicos deberá ceñirse a las conductas de apoderamiento con desplazamiento físico de mensajes de telefax o de mensajes de correspondencia electrónica o informática, pero imprimidos todos ellos fuera del sistema, puesto que la interceptación, grabación o reproducción ilícita de carácter electrónico de estos mensajes, por ejemplo, vulnerando el **password** o clave de acceso electrónica, quedará abarcada por la siguiente modalidad típica.

III) En cuanto al apoderamiento de los «**soportes informáticos**», se verificará, en su primera mención, cuando el sujeto activo del delito se lleve el disquete o el CD-ROM donde se contuviere el secreto

IV) Y, por último, se contempla una cláusula de cierre «**u otros objetos que se refieran al secreto**», que evite cualquier posible laguna; de este modo el apoderamiento podrá recaer sobre **cualquier otro objeto que se refiera al secreto**, ya sea de carácter sonoro o audiovisual, como, por ejemplo, cintas

que es sólo de lectura, la memoria RAM cubre, a su vez, diferentes tipos de memoria electrónica. A medida que el usuario opera se almacenan en esta memoria los datos con los que trabaja. Sin embargo, como dicha memoria es volátil, cuando se apaga el ordenador, se pierde la información contenida en ella, a menos que se haya grabado en disco, cinta u otro soporte (así, vid. GUIBOURG, R.A./ALENDE, J.O./CAMPANELLA, E.M., **Manual de informática jurídica**, Buenos Aires, 1996, p. 45). Por tanto, cualquiera de estas memorias es idónea como soporte de los datos.

de casete o de vídeo, maquetas, prototipos o cualquier otro soporte que lo contenga¹²⁶⁷.

En conclusión, el apoderamiento de secretos empresariales se verificará tanto con la aprehensión inmaterial de la información como mediante el apoderamiento físico de los documentos o soportes que la contengan.

Sin duda alguna, esta previsión típica ha supuesto la introducción de una figura novedosa en el vigente código penal español, puesto que el apoderamiento de secretos de empresa constituía en el ACP una importante laguna de punibilidad. Ahora bien, la configuración de la acción típica del delito de **apoderamiento** de secretos de empresa, al margen de su tradicional vinculación a delitos de apoderamiento material, cuyas figuras típicas se hallan concebidas para la protección de cosas corporales, aprehensibles materialmente y susceptibles de desplazamiento¹²⁶⁸, está todavía lastrada por su asentamiento originario entre los delitos sobre el descubrimiento y revelación de secretos¹²⁶⁹. A nuestro parecer, el apoderamiento de datos, documentos o soportes referidos al secreto parece arbitrarse aún sobre la tutela de **secretos documentales** o de soporte

¹²⁶⁷ Así, el legislador prevé una cláusula concursal (art. 278.3 CP) para el supuesto en que la conducta realizada suponga el apoderamiento o destrucción de los soportes informáticos. Como se ha expuesto en otro lugar, se trata de una referencia innecesaria y perturbadora. De una parte, los diferentes bienes jurídicos tutelados en este precepto y en el delito de apoderamiento (hurto o robo) o destrucción (daños informáticos) de los soportes permiten acudir a las reglas concursales genéricas. De otra, el precepto restringe injustificadamente su ámbito a los soportes informáticos, quedando excluidos todos los demás (así, vid. MORALES PRATS, F./MORÓN LERMA, E., en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios al Nuevo Código Penal**, Pamplona, 2ª ed., 2001, pp. 1288-1289).

¹²⁶⁸ Así, GUTIÉRREZ FRANCÉS, M.L., "Notas sobre la delincuencia informática...", en ARROYO ZAPATERO, L./TIEDEMANN, K., **Estudios de derecho...**, *op. cit.*, p. 188.

¹²⁶⁹ MASSAGUER FUENTES, J.J., "Los secretos industriales y comerciales y su transmisión: régimen jurídico", en FONT GALÁN, J.I./NAVARRO CHINCHILLA, J.J./VÁZQUEZ GARCÍA, R.J., **Derecho de la propiedad industrial, Cuadernos de Derecho y Comercio**, Monográfico, 1994, p. 183.

análogo, que recuerda a la anacrónica estructura del art. 497 ACP, que castigaba al que «para descubrir los secretos de otro **se apoderase** de sus papeles o cartas»¹²⁷⁰.

En este sentido, se corre el peligro de identificar como dato clave de estas figuras el soporte del secreto en vez de la información que lo conforma. De ahí que quizá devenga más adecuado el empleo de cualquier otro término que haga hincapié en el aspecto relevante de esta modalidad típica —el acceso ilícito a la información—y no en otras cuestiones como el soporte del objeto, sin perjuicio de que la diferenciación de las diversas modalidades en que puede traducirse el acceso ilícito pueda, asimismo, captar la divergencia de desvalor y, por tanto, tener relevancia en orden a la determinación de la gravedad de la pena¹²⁷¹.

En suma, pues, se revelará adecuada la configuración que aprehenda acertadamente uno de los criterios que define el ámbito de lo punible en esta modalidad de ataque, que se asienta en la **adquisición o acceso al secreto, acometido de forma indebida, esto es, sin actividad propia**. A continuación, conviene abordar el otro de los criterios que contribuye a delimitar el ámbito típico en esta modalidad comisiva, a saber, el elemento subjetivo.

1.2. El elemento subjetivo como criterio delimitador del alcance de esta modalidad de acción: el ánimo de descubrir el secreto.

Para concluir la delimitación de lo que constituye el ámbito de lo punible a partir del examen y análisis de las acciones típicas, por lo que

¹²⁷⁰ Para un análisis crítico de la técnica empleada en el antiguo art. 497 ACP, vid. MORALES PRATS, F., *La tutela penal de la intimidad*:..., *op. cit.*, pp. 176 y ss.

¹²⁷¹ Vid., en este sentido, *infra*, la recapitulación y conclusión crítica al acceso ilícito, epígrafe 2.3.

atañe al apoderamiento –y, en realidad, a todas las modalidades de acceso ilícito-- es necesario acudir al elemento subjetivo, puesto que la parte objetiva del tipo queda dibujada a partir de aquél.

En efecto, para poder determinar si estamos en presencia de apoderamientos típicos, se revela determinante la función restrictiva que ejercerá el elemento subjetivo del injusto, cuya exégesis --que puede adoptar una doble vía o vertiente-- asume, pues, una notable importancia.

De una parte, el elemento subjetivo cifrado en el ánimo de descubrir un secreto de empresa, puede interpretarse como sinónimo de **intención de revelar**, siguiendo la línea interpretativa sostenida a propósito del art. 499 ACP y la formulada respecto del art. 278.1 CP, en la reciente STS de 16 de febrero de 2001¹²⁷². De ser así, podría decirse que el que sustrae un programa informático, al que tiene acceso legítimamente, con intención de revelarlo o divulgarlo, al margen de trascendentales problemas probatorios, cometería un acto típico.

Sin embargo, con arreglo a la segunda opción interpretativa del elemento subjetivo, en la que el ánimo de descubrir un secreto se considera como equiparable a la **intención de conocimiento del mismo**¹²⁷³, no parece

¹²⁷² STS 16 de febrero 2001 (LL, nº 3281).

¹²⁷³ En este caso, ya que el efectivo descubrimiento del secreto no es una condición típica, sino sólo un elemento de engarce de la siguiente modalidad prevista en el art. 278.2 o, en su caso, en el art. 279.1 CP --dependiendo de cómo sea calificado el acceso--, no parece compatible que la interpretación como ánimo de conocer deba conducir a su descubrimiento efectivo y, por ende, a la aplicación de otra secuencia típica, según se argumenta en la STS 16 febrero 2001 (fundamento de derecho único, párrafo tercero). Es decir, es posible que un trabajador sustraiga y se lleve a su domicilio un disquete en el que se halla registrada una concreta técnica de gestión de la cartera de clientes (con información sobre sus preferencias, descuentos, antigüedad, etc.), sin tener conocimiento efectivo de la misma, pero sabiendo que se halla en el disquete. En cualquier caso, e independientemente de cuál haya sido la finalidad última (revelar, explotar, ceder, etc.), dicha finalidad reclama conceptualmente la previa de conocer el secreto, sin cuyo descubrimiento parece difícil que puedan acometerse las otras posibles tendencias

posible sostener que la conducta devendría, en este caso, típica, al no ejecutarse la conducta informada por esta específica tendencia¹²⁷⁴. En efecto, un acceso con autorización, esto es, llevado a cabo no en debida forma sino con intención de divulgar o de explotar el secreto --en definitiva, de usarlo de modo contrario a las reglas de la competencia--, no puede ser entendido como un apoderamiento típico sin colisionar con el elemento subjetivo, entendido como ánimo de conocer el secreto.

Así pues, dependiendo del contenido interpretativo que se otorgue al elemento subjetivo del injusto, el apoderamiento de soportes u objetos referidos al secreto con autorización pero ejecutándolo de una forma indebida, devendrá una conducta típica o, por el contrario, impune.

A nuestro parecer, la inteligencia del elemento subjetivo relativo al ánimo de descubrir el secreto como equiparable al ánimo de divulgarlo cobraba pleno sentido en la regulación prevista en el art. 499 ACP, que castigaba al empleado que descubría --esto es, revelaba-- los secretos de su principal. Sin embargo, esa significación preñada de sentido en el anterior código decae por completo en el vigente. En efecto, las modalidades típicas incriminadas en uno y otro código son distintas --en el art. 499, revelar y en el art. 278.1, apoderarse, acceder--, de forma que una interpretación lógico-sistemática del elemento subjetivo aconseja su entendimiento como ánimo de conocer y no de divulgar.

Así pues, **de lege lata**, resulta postulable la segunda de las opciones reseñadas, que lo equipara al ánimo de conocer, aunque, como se verá, dé

ulteriores. En suma, en este caso, si no se tenía autorización se trataría de un supuesto normal de apoderamiento de un secreto de empresa en soporte informático.

¹²⁷⁴ A salvo de que se considere iniciada la ejecución de la revelación, difusión o cesión (ex art. 278.2 o ex art. 279.1 CP, según sea calificado en el caso concreto el acceso) o la utilización en provecho propio (ex art. 279.2 CP).

lugar a lagunas indeseables y el elemento subjetivo devenga, en esa medida, necesitado de reforma.

Retomando, pues, la resolución jurídica del ejemplo, frecuentemente suscitado en la práctica, o se lleva a cabo una interpretación forzada de todo el precepto a fin de otorgar cobertura típica a esa conducta, que no parece deseable o la concreción que se ha hecho del elemento subjetivo impide considerar el apoderamiento de un secreto que ya se conoce, con la intención de divulgarlo, como una conducta subsumible en esta modalidad típica.

Desde luego, cuestión distinta será el enjuiciamiento de la parte subjetiva y del posible inicio de ejecución del art. 279.1 CP, que castiga la difusión, revelación o cesión de un secreto por quien tiene obligación de guardar reserva. En este momento, se trata de analizar si la conducta descrita merece sanción ya como espionaje o adquisición ilícita del secreto. Esto es, como primera etapa o estadio previo a la posterior difusión, revelación, cesión o aprovechamiento del secreto, que el legislador sí ha previsto como conductas sancionables¹²⁷⁵. Y a tenor de los inconvenientes expuestos, parece que, según la dicción del precepto, no sería un supuesto de acceso, adquisición o espionaje punible.

Sin embargo, a nuestro juicio, el apoderamiento del secreto con la intención de aprovecharse del mismo o de utilizarlo indebidamente constituye una circunstancia determinante de la deslealtad de la conducta, que debería ser tomada en cuenta en la tipificación de estos preceptos. Desde luego, ello supone una anticipación de la tutela no exenta de problemas, pero quizá aconsejable a tenor de las peculiares características del objeto del delito y de la acción. Se trata de información sensible y fácilmente

¹²⁷⁵ **Poner ejemplo de superlopez. Esquema y prensa**
545

expugnable en cuanto bien económico sustentado, fundamentalmente, en el mantenimiento de la reserva.

Al respecto, es oportuno advertir que el ordenamiento alemán ha incorporado una descripción amplia del elemento subjetivo que permite no eludir ninguno de estos supuestos. Así, se reclama que el autor obre con finalidad competitiva, en beneficio propio o a favor de un tercero o con la intención de perjudicar al propietario de la empresa, lo que permite incriminar conductas de aseguramiento del secreto sin autorización acometidas con esa finalidad (§ 17, II, 1 UWG).

Este elemento subjetivo coincide, básicamente, con el previsto en la LCD española, con arreglo a la cual la conducta sería, con certeza, susceptible de reproche. En efecto, constituiría un supuesto de adquisición de secretos por un procedimiento indebido, al haber sido llevada a cabo la adquisición con la intención de divulgar o explotar y, por tanto, con el ánimo de obtener provecho propio, o de un tercero o de perjudicar al titular del secreto (ex art. 13.2 y 3 LCD).

Desde luego, en esta línea puede considerarse integrada la propuesta de GUTIÉRREZ FRANCÉS que, inspirándose en la incriminación del espionaje informático previsto por el ordenamiento alemán¹²⁷⁶, postula como hipotético modelo la siguiente descripción: «Quien sin autorización se procure a sí mismo o procure a otros datos...». Así, a juicio de esta autora, lo relevante, según esta fórmula, es la obtención de los datos y no la forma concreta de obtenerlos¹²⁷⁷. Sin duda, se trata de una fórmula acertada,

¹²⁷⁶ Así, vid. § 202 a StGB, regulador del espionaje de datos, que establece: «1. Quien sin autorización se procure a sí mismo o procure a otros datos especialmente asegurados contra ilícitas intromisiones, será castigado...».

¹²⁷⁷ GUTIÉRREZ FRANCÉS, M.L., “Notas sobre la delincuencia informática...”, en ARROYO ZAPATERO, L./TIEDEMANN, K., *Estudios de derecho...*, *op. cit.*, p. 197.

aunque al respecto conviene efectuar varias matizaciones. De una parte, la cláusula «sin autorización» es perfectamente aceptable, puesto que, como se ha señalado, la adquisición de secretos es indebida cuando quien la realiza no guarda una relación con el titular que autorice su ejecución. Ahora bien, a tenor del bien jurídico protegido en estos preceptos, la competencia por el propio esfuerzo y, en concreto, el interés económico del empresario en mantener la reserva sobre ciertas informaciones fruto de su propia actividad, parece que lo realmente determinante será la **adquisición ilícita**, esto es, la obtención de la información sin esfuerzo ni actividad propia, que, por tanto, reviste matices propios que pueden contribuir a perfilar lo que sería una mera **adquisición sin autorización**. Precisamente, este criterio obtenido del derecho de la competencia desleal es el que, proyectado a los medios comisivos, determinará cuándo estas conductas se convierten en punibles. De ahí que, en puridad, el que obtiene el secreto por ingeniería inversa o fruto de sus propias investigaciones o, incluso, por azar, no lleve a cabo una apropiación ilícita, independientemente de que guarde o no una relación con el titular que le **autorice** a dicha adquisición¹²⁷⁸. Por otro lado, sólo a partir de este presupuesto, puede interpretarse la opinión manifestada por GUTIÉRREZ FRANCÉS, en cuya virtud lo relevante es la obtención de los datos y no la forma concreta de obtenerlos¹²⁷⁹. Esto es, la importancia de la forma de obtención de los datos es tan notable que se erige en el **criterio o circunstancia que permite formular el reproche de deslealtad a la conducta**, y sólo a partir de esta inicial ilicitud determinante de la deslealtad, puede

¹²⁷⁸ De ahí que el que obtiene la fórmula de la coca-cola por ingeniería inversa o el que averigua el proceso productivo de Inditex por medio de la observación y de sus propias investigaciones o, incluso, el que descubre una nueva utilización de un producto ya conocido, por simple azar, no cometa actos delictivos.

¹²⁷⁹ En este sentido se pronuncia, también, PRATS CANUT, J.M., “Descubrimiento y revelación de secretos de empresa en el Código Penal de 1995”, en **Delitos relativos a la propiedad industrial, al mercado y a los consumidores**, CDJ, CGPJ, 1997, p. 189, al afirmar que «lo relevante es el apoderamiento y no el medio empleado».

considerarse que la concreta forma –ilícita en todo caso—de acceso a los mismos no es relevante.

Aun así, no parece compatible del todo esta última reflexión, puesto que, como se ha manifestado, las diferentes modalidades en que puede acometerse un apoderamiento ilícito pueden revestir diversa insidiosidad para el bien jurídico y, en esa medida, quizá convenga que el legislador las diferencie en la dicción del tipo y, en rigor, las tenga en cuenta en la determinación de la pena.

En conclusión, pues, la circunscripción de lo punible en este ámbito parece reclamar un elemento de tendencia subjetiva de contornos más amplios que el actualmente previsto (ánimo de descubrir), cuya presencia permita seleccionar las conductas con capacidad de afección sobre el bien jurídico, aunque suponga, en cierta medida, un adelantamiento de la tutela penal. En esta lógica, se estima adecuada la opción prevista por la LCD española, en cuya virtud uno de los criterios determinantes de la adquisición ilícita de los secretos descansa en que sean acometidos con **el ánimo de obtener provecho, propio o de un tercero o de perjudicar al titular del secreto**. El criterio adicional a estos ánimos, que incorpora la UWG alemana, cifrado en el ánimo de competir, se revela, a nuestro juicio, superfluo e innecesario. De una parte, parece consustancialmente incluido ya en alguno de los propuestos y, de otra, la propia restricción del bien jurídico, determinará que las conductas que no vayan a proyectarse en la esfera competitiva y, por tanto, no tengan capacidad de ofender el bien jurídico protegido, se vean marginadas del ámbito penal, como exige el principio de ofensividad o de insignificancia¹²⁸⁰.

¹²⁸⁰ La interpretación del objeto jurídico de protección –el interés económico-- y del propio instrumento –el secreto de empresa-- sobre el que dicha protección se arbitra ha sido acometida desde el derecho de la competencia desleal. Ello ha permitido identificar con claridad los intereses protegidos en el ámbito penal, cifrados en la tutela del interés económico en mantener la reserva sobre ciertas informaciones, como modo de preservar

De ahí que, según se expuso en la interpretación del concepto de esta modalidad de acción, sean, esencialmente, dos los criterios que, desde distintas perspectivas –el bien jurídico y el elemento subjetivo--, contribuyen a restringir y delimitar el ámbito de lo punible. En concreto, de una parte, la inteligencia del apoderamiento como una conducta acometida indebidamente, esto es, con aprovechamiento del esfuerzo ajeno y, de otra, que dicha acción sea guiada por el ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto.

Esta definición del ámbito propio de las conductas de apoderamiento, como primera y básica modalidad de ataque, permite, en este momento, estudiar la estructura de esta acción que se halla parcialmente recogida en el artículo 278.1, primer apartado del CP.

1.3. Estructura típica: delito de mera actividad o delito de resultado.

En cuanto a la **estructura típica** que debe atribuirse a la conducta de apoderamiento¹²⁸¹, que se encuentra prevista en la primera secuencia del artículo 278.1 CP, especial complejidad plantea la decisión acerca de si se corresponde con la de los delitos de simple conducta del autor o con la de los delitos de resultado. Desde luego, parece que cualquier opción se halla directamente relacionada con el concepto de resultado que se adopte. Así,

los resultados fruto del propio esfuerzo y fomentar, así, el avance y el progreso también mediante el propio esfuerzo, y sin apropiación indebida del esfuerzo ajeno. De modo que, en estos delitos, la protección del interés económico del empresario no podrá proyectarse cuando no se produzca esa injerencia del tercero en la esfera de libertad ajena de ejercer una actividad económica.

¹²⁸¹ En el ámbito de las diversas modalidades de conducta que integran el acceso ilícito al secreto (apoderamiento, interceptación y otras conductas ilícitas asimilables), no habrá grandes diferencias por lo que se refiere a la estructura típica que se analiza.

destinado a tal fin conviene repasar escuetamente las posiciones que pueden mantenerse al respecto.

a) Desde una concepción del resultado en sentido naturalístico, esto es, entendido como el efecto exterior de la conducta espacio-temporalmente separable de la misma¹²⁸², que suele cifrarse en el menoscabo, destrucción o puesta en peligro de bienes jurídicos tangibles o materiales¹²⁸³, parece difícil equiparar la estructura del apoderamiento de secretos de empresa para descubrirlos a la de los delitos de resultado material, puesto que ni es necesario que éste se produzca ni el bien jurídico es susceptible de menoscabo físico.

b) Desde un entendimiento del resultado típico como suceso distinto de la acción y separable de ésta al menos mentalmente¹²⁸⁴, se califica este delito como un delito de resultado¹²⁸⁵, al entender el apoderamiento como capacidad efectiva del agente de disponer de los datos u objetos de la acción¹²⁸⁶. Sin duda, el apoderamiento implica necesariamente la disposición de los datos, aunque el sujeto no los comprenda y, por tanto, no haya tomado efectivamente conocimiento de los mismos. Ahora bien, parece que no resulta tanto un posible «efecto de la acción en el sentido de suceso causado por la acción típica»¹²⁸⁷, concebible, pues, como resultado de la

¹²⁸² Así, OCTAVIO DE TOLEDO Y UBIETO, E./HUERTA TOCILDO, S., **Derecho penal, Parte general, op. cit.**, pp. 72-73.

¹²⁸³ QUINTERO OLIVARES, G., en QUINTERO OLIVARES, G./MORALES PRATS, F./PRATS CANUT, J.M., **Manual de derecho...**, op. cit., p. 317.

¹²⁸⁴ GÓMEZ BENÍTEZ, J.M., **Teoría jurídica del delito, Derecho penal, Parte general**, Madrid, 1992, pp. 167 y ss.

¹²⁸⁵ MORENO CÁNOVAS, A./RUIZ MARCO, F., **Delitos socioeconómicos, op. cit.**, p. 127.

¹²⁸⁶ MORENO CÁNOVAS, A./RUIZ MARCO, F., **ibidem**.

¹²⁸⁷ Ésta es la línea de razonamiento seguida por CARRASCO ANDRINO, M.M., en **La protección penal...**, op. cit., p. 208, respecto del art. 279.1, siguiendo a LAURENZO

acción, sino que **se trata de la propia acción**, puesto que el último acto de apoderamiento o de acceso a la información implica ya, en ese mismo momento, su capacidad de disposición sobre ellos. Sólo se encuentran dos posibles vías de argumentación que impidan lo anteriormente expuesto. En primer lugar, entender efectivamente la disposición como suceso causado por la acción y, por tanto, como resultado típico del apoderamiento, en cuanto consecuencia próxima y estrechamente vinculada a la acción del sujeto pero separable mentalmente aunque sea instantáneamente, lo que, quizá, supondría, **a fortiori**, vaciar de contenido la categoría de los delitos de mera actividad. Y, en segundo lugar, entender la disposición de los datos como resultado distinto del acceso en la medida en que se conciba la posibilidad de que ambas acciones asuman un contenido diverso. Así, puede pensarse en el caso de que un sujeto se apodera de un disquete que contiene un documento cifrado, que se identifica, por ejemplo, con la estrategia de mercado del siguiente trimestre, pero cuyo contenido sólo se intuye por el título del documento. Posteriormente, cuando se descodifica se comprueba que no es así, puesto que contiene otro tipo de información o porque en el proceso de descodificación se han producido daños en el archivo y, en esa medida, el apoderamiento de los datos por parte del sujeto no ha conllevado la efectiva disposición de los mismos. En el primero de los supuestos, el debate se centraría en el ámbito del objeto, al tratarse bien de una conducta atípica por ausencia de objeto (la información es un artículo de prensa publicado el día anterior sobre estrategias de mercado) o bien de un supuesto de error de tipo con distinta relevancia, según se trate. En el segundo caso, se trataría de un supuesto en el que el sujeto ha llevado a cabo una conducta consumada, puesto que con el mero apoderamiento ha tenido una efectiva disposición de los datos y cuya posterior inutilización, por tanto, se aleja ya de cuestiones atinentes a la órbita típica.

COPELLO, P., **El resultado en derecho penal**, Valencia, 1992, pp. 113 y ss., quien, a su vez, cita a HORN.

c) Asimismo, es posible concebir el resultado como un efecto, material o ideal, consecuencia de la conducta y distinto de la misma, generalmente posterior pero a veces simultáneo a ella¹²⁸⁸. Según esta concepción, aunque el resultado no se limita a su entendimiento en sentido puramente naturalístico, parece que no se conforma con entender el resultado como un mero suceso separable mentalmente de la acción, sino que requiere algún tipo de proyección adicional. Así, por ejemplo, el delito de injurias es concebido como un delito de resultado, pero en él se requiere, como necesario para que se cumpla el tipo, el conocimiento por parte del tercero como un proceso autónomo frente a la acción del autor¹²⁸⁹. Con arreglo pues a esta concepción, el apoderamiento de secretos de empresa no reclama ni engendra ningún proceso autónomo de efectiva disposición, conocimiento y, en suma, implicación de tercero, por lo que su estructura se correspondería con la de los delitos de mera actividad.

A la complejidad expuesta, debe añadirse la inherente a la singular naturaleza de estos delitos. Como advierte QUINTERO OLIVARES, la naturaleza de los bienes jurídicos tutelados penalmente resulta determinante en el modo o clase de ataques posibles que pueden vulnerarlo y, por ello, también en la estructura típica que los sanciona¹²⁹⁰. En este sentido, la naturaleza del bien jurídico protegido por estos preceptos, que estriba en el interés económico del empresario en mantener la reserva de ciertas informaciones y que se asienta en un bien económico –el secreto de empresa-- extraordinariamente sensible y expugnable, al depender su propia

¹²⁸⁸ LUZÓN PEÑA, D.M., *Curso de derecho penal, Parte general, I*, Madrid, 1996, p. 307.

¹²⁸⁹ ROXIN, C., *Derecho penal, Parte general, T. I, Fundamentos. La estructura de la teoría del delito*, 2ª ed. trad. por LUZÓN PEÑA/DÍAZ Y GARCÍA CONLLEDO/DE VICENTE REMESAL, Madrid, 1999, p. 328.

¹²⁹⁰ QUINTERO OLIVARES, G., en QUINTERO OLIVARES, G./MORALES PRATS, F./PRATS CANUT, J.M., *Manual de derecho...*, *op. cit.*, pp. 315 y 317.

existencia de la situación de reserva, de la que deriva ese valor económico que su posesión atribuye al empresario, deviene susceptible de múltiples y distintas modalidades de ataque (graves pérdidas que provoquen la quiebra, desorganización de la empresa, disminución del círculo de clientela, etc.) que parecen difícilmente concebibles como un suceso o efecto exterior, vinculado al apoderamiento de cierta información. Por otra parte, como se sabe, el bien económico sobre el que se sustenta el bien jurídico es de naturaleza intangible e inmaterial, lo que contribuye a que sea complejo encuadrar estas figuras delictivas en categorías surgidas para captar bienes de distinta configuración y naturaleza y, en esa medida, contribuye también a que dichas categorías, salvaguardando las garantías, pierdan rigidez conceptual en ciertos bienes jurídicos cuya protección se arbitra sobre elementos de nueva conformación y frente a modalidades de ataque de reciente aparición.

En conclusión, pues, en la **estructura típica** de esta primera secuencia del precepto se reclama una conducta de apoderamiento con intención de descubrir un secreto empresarial, sin necesidad de un ulterior resultado, material o ideal, distinto del mero apoderamiento. Esto es, ni se requiere el efectivo descubrimiento del secreto (que sólo actuará como elemento de engarce respecto a la modalidad prevista en el artículo 278.2 CP, de difusión, revelación o cesión de los secretos descubiertos), ni ningún proceso de conocimiento o de disponibilidad del secreto en la esfera de un tercero como proceso autónomo de la conducta del autor, ni, en suma, ningún resultado, posterior o simultáneo, consecuencia de la conducta. Se trata, pues, a nuestro parecer, de un **delito de mera conducta o de mera o pura actividad**¹²⁹¹.

¹²⁹¹ Desde luego, como advierten COBO DEL ROSAL, M./VIVES ANTÓN, T.S., **Derecho penal, op. cit.**, p. 441, n. 38, resulta inadecuado denominar a los delitos de mera actividad delitos formales, ya que el injusto típico no es nunca una mera forma (fórmula) vacía, sino que comporta, en todo caso, un contenido lesivo.

Precisamente, atendiendo a la especificidad del bien jurídico y a la fragilidad del objeto material, el legislador ha estructurado esta figura típica como un **delito de consumación anticipada**, incorporando al tipo un elemento subjetivo del injusto adicional al dolo y consistente en el ánimo de descubrir un secreto de empresa. Así, se trata de un **delito mutilado de dos actos**, cuya consumación reclama únicamente la realización de la primera conducta de apoderamiento doloso de un secreto empresarial con el ánimo de descubrirlo, bastando al efecto la mera constatación de que el agente actúa animado por esta intención. Se adelanta pues el momento de la consumación al acto de apoderamiento intencional, sin que se requiera la efectiva toma de conocimiento del secreto de empresa para la perfección típica¹²⁹². Como se ha dicho ya, el descubrimiento del secreto actúa a modo de elemento de engarce con el tipo agravado de difusión, revelación o cesión del secreto descubierto (art. 278.2 CP), que, al presentar una estructura típica doble o de delito compuesto, reclama la previa verificación de la conducta del tipo básico analizado (art. 278.1, primer párrafo CP) y de la secuencia de nexos, representada por la toma de conocimiento del secreto.

¹²⁹² Así, BAJO FERNÁNDEZ, M., *Derecho penal económico aplicado...*, *op. cit.*, p. 307 y BAJO FERNÁNDEZ, M./SUÁREZ GONZÁLEZ, C., en BAJO FERNÁNDEZ, M./PÉREZ MANZANO, M./SUÁREZ GONZÁLEZ, C., *Manual de derecho penal, Parte especial...*, *op. cit.*, p. 382; BERDUGO GÓMEZ DE LA TORRE, I., “La tutela de la competencia...”, en *La reforma penal*, *op. cit.*, p. 418; CARBONELL MATEU, J.C./GONZÁLEZ CUSSAC, J.L., en AA VV (Coord. VIVES ANTÓN, T.S.), *Derecho penal, Parte especial*, 3ª ed., Valencia, 1993, p. 765; MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, *op. cit.*, pp. 74-75; SUÁREZ GONZÁLEZ, C., en AA VV, (RODRÍGUEZ MOURULLO, G., Dir.), *Comentarios al Código Penal*, Madrid, 1997, p. 803; MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos*, *op. cit.*, p. 126; GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal*, *op. cit.*, p. 799; PRATS CANUT, J.M., “Descubrimiento y revelación de secretos de empresa en el Código Penal de 1995”, en *Delitos relativos a la propiedad industrial, al mercado y a los consumidores*, CDJ, CGPJ, 1997, p. 186.

No se puede revelar o difundir lo que previamente no se ha conocido de forma efectiva¹²⁹³.

1.4. Momento de la consumación.

Desde la perspectiva de la modalidad o de la intensidad de ataque al bien jurídico protegido, la conducta de apoderamiento constituye un **delito de peligro**, puesto que no se requiere la lesión del interés económico del empresario o la producción de un perjuicio económico, difícilmente mensurable en este ámbito de intereses. Si lo anteriormente expuesto parece incontrovertible, determinar si estamos en presencia de una estructura de peligro concreto o de peligro abstracto reviste mayor complejidad.

Como se sabe las diversas modalidades que reviste la relación entre la conducta y el bien jurídico dan lugar a la distinción entre delitos de peligro concreto y delitos de peligro abstracto, tradicionalmente admitida pero, como advierte TERRADILLOS BASOCO, aún con diferencias terminológicas de no escasa significación¹²⁹⁴.

Los delitos de peligro concreto exigen que la acción del sujeto activo cause un resultado consistente en la creación de un concreto peligro de lesión para el bien tutelado, de modo que, al ser el peligro un elemento del

¹²⁹³ MORALES PRATS, F/MORÓN LERMA, E., en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios al Nuevo Código Penal**, Pamplona, 2ª ed., 2001, p. 1282; MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte especial, op. cit.**, p. 76.

¹²⁹⁴ TERRADILLOS BASOCO, J., **Derecho penal..., op. cit.**, p. 53. En efecto, las diferencias que median en estas categorías trascienden lo puramente terminológico, de forma que el empleo de unas u otras implica asimismo un ámbito distinto, lo que coadyuva la complejidad inherente a la materia.

tipo, para que pueda hablarse de realización típica, se exige la demostración de que se produjo efectivamente la situación de riesgo¹²⁹⁵.

Los delitos de peligro abstracto se integran con la presencia de la acción del sujeto activo, siendo suficiente la comprobación de una peligrosidad general de la misma para algún bien jurídico, sin que se requiera, por tanto, concreción alguna de un peligro efectivo creado por la acción.

Fruto del enjuiciamiento crítico al que han sido sometidos los delitos de peligro abstracto por implicar una presunción de mera peligrosidad formal¹²⁹⁶, inaceptable desde la vigencia del principio de ofensividad y desde un concepto de antijuridicidad material, que constriñe a la afirmación de la constitucionalidad de la ilicitud de cualquier conducta carente de lesividad, la doctrina ha propuesto criterios correctores de una concepción de los delitos de peligro abstracto como delitos carentes de contenido de injusto material. A tal efecto, se ha propuesto la formulación de una distinción de los mismos en otros términos o la creación de categorías, en cierto modo, intermedias.

Así, mejor que afirmar que en los delitos de peligro abstracto no se precisa un efectivo peligro, es distinguir estas categorías con arreglo a los siguientes términos: en los delitos de peligro concreto el tipo requiere como resultado de la acción la **proximidad** de una **concreta** lesión, mientras que en los delitos de peligro abstracto no se exige tal **resultado** de proximidad de

¹²⁹⁵ Así, vid., entre otros, TERRADILLOS BASOCO, J., *Derecho penal...*, op. cit., p. 53 y MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte general*, op. cit., p. 107.

¹²⁹⁶ Así, vid., entre otros, TORÍO LÓPEZ, A., "Los delitos del peligro hipotético (Contribución al estudio diferencial de los delitos de peligro abstracto)", en *ADPCP*, 1981, pp. 826 y ss.; OCTAVIO DE TOLEDO Y UBIETO, E./HUERTA TOCILDO, S., *Derecho penal, Parte general*, op. cit., p. 165; COBO DEL ROSAL, M./VIVES ANTÓN, T.S., *Derecho penal*, op. cit., pp. 301-302.

una lesión de un concreto bien jurídico¹²⁹⁷. Por consiguiente, para evaluar el riesgo en estos últimos se utilizará un juicio **ex ante** acerca de la peligrosidad de la acción, a diferencia de lo que ocurrirá en los delitos de peligro concreto, en los que habrá que recurrir a una perspectiva **ex post** para enjuiciar el resultado de peligro¹²⁹⁸.

A fin de solventar la peligrosidad formal de los puros delitos de peligro abstracto, TORÍO LÓPEZ propuso una categoría nueva, denominada **delitos de peligro hipotético**¹²⁹⁹ que integró dentro de los delitos de peligro abstracto, en tanto no precisan, a diferencia de los delitos de peligro concreto, de un peligro real y efectivo para el bien jurídico como un **plus** ulterior a la acción. En ellos es necesaria, aunque suficiente, la ejecución de una acción peligrosa apta o idónea para producir un peligro para el bien jurídico protegido, como elemento material integrante del tipo de delito¹³⁰⁰. En estos delitos, en los que la tipicidad presupone el juicio **ex ante** de que el comportamiento puede originar un peligro para el bien jurídico, el juez además deberá verificar si en la situación concreta ha sido posible un mínimo contacto entre acción y bien jurídico, en cuya virtud hubiera podido producirse un peligro efectivo para éste¹³⁰¹.

¹²⁹⁷ Así, vid. MIR PUIG, S., *Derecho penal, Parte general, op. cit.*, p. 209.

¹²⁹⁸ Así, vid. MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte general, op. cit.*, p. 108.

¹²⁹⁹ TORÍO LÓPEZ, A., "Los delitos del peligro hipotético (Contribución al estudio diferencial de los delitos de peligro abstracto)", en *ADPCP*, 1981, pp. 828 y ss. y 838 y ss.

¹³⁰⁰ A estos delitos se hace referencia con otras denominaciones como «delitos de peligro posible» (GALLAS), «delitos de peligro abstracto-concreto» (SCHRÖDER), «delitos de peligro potencial» (KELLER), entre otras. Como se ha manifestado ya, estas divergencias trascienden lo puramente terminológico. De ahí que en esta investigación se recurra a la denominación específica de «delitos de peligro hipotético», entendida en el modo originalmente formulado por TORÍO.

¹³⁰¹ Así, vid. TORÍO LÓPEZ, A., "Los delitos del peligro hipotético...", *op. cit.*, pp. 840 y 846.

Pues bien, teniendo presente el hondo debate suscitado sobre la legitimidad de estas estructuras de peligro, con carácter general, en el ámbito del derecho penal económico¹³⁰², pero en cuyo estudio no puede ahondarse, conviene proceder ya al análisis de la estructura que reviste la modalidad típica ahora analizada, relativa al apoderamiento de secretos de empresa.

En este sentido, según advierte TERRADILLOS BASOCO¹³⁰³, la legitimación constitucional y la funcionalidad político-criminal de la decantación legislativa por las estructuras de peligro ha de valorarse desde la perspectiva de la importancia y características del bien jurídico que se trata de proteger. Así pues, como reclama MORALES PRATS, en su tipificación debe partirse de **criterios materiales de desvalor**, que no tomen en consideración en mayor medida la graduación del peligro desde el punto de vista de la acción, sino **la afección de los bienes jurídicos** en juego, puesto que desde esta perspectiva puede detectarse la necesidad de anticipar la intervención del derecho penal, a la vista de las fuentes de peligro para el bien jurídico y de la sensibilidad del bien jurídico necesitado de protección¹³⁰⁴.

En este caso, el bien jurídico protegido se cifra en el interés económico del empresario en mantener la reserva. Ahora bien, el bien jurídico se halla estrechamente vinculado al objeto material, esto es, al

¹³⁰² Vid., al respecto, entre una profusa literatura, TERRADILLOS BASOCO, J., **Derecho penal...**, *op. cit.*, pp. 51 y ss; MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte general**, *op. cit.*, p. 112 y ss; KINDHÄUSER, U.K., "Acerca de la legitimidad de los delitos de peligro abstracto en el ámbito del derecho penal económico", en **Hacia un derecho penal económico europeo. Jornadas en honor del Profesor Klaus Tiedemann**, *op. cit.*, pp. 441 y ss.

¹³⁰³ TERRADILLOS BASOCO, J., *op. ult. cit.*, p. 51.

¹³⁰⁴ MORALES PRATS, F. "Técnicas de tutela penal de los intereses difusos", en **Intereses difusos y derecho penal**, *op. cit.*, p. 78.

secreto de empresa, que se configura como un bien económico extremadamente sensible. En efecto, el elemento esencial y sustentáculo de ese interés económico estriba en el mantenimiento de la reserva, de la que deriva el valor económico que proporciona la información. Obsérvese que, por tanto, el mantenimiento de la reserva, que atribuye ese monopolio fáctico, se proyecta sobre informaciones económicas sensibles. Es decir, no se trata de bienes materiales recuperables en su esencia, sino que, por el contrario, una vez descubierto el secreto, generalmente, se produce la destrucción o menoscabo irreparable del bien económico en sí. Además, el apoderamiento de la información no permite su posterior restitución, puesto que, una vez introducida en la esfera de disposición del sujeto activo, éste puede, potencialmente, hacer uso de ella en cualquier momento, de modo que, casi con toda certeza, es irre recuperable en su indemnidad funcional.

En suma, pues, la especial sensibilidad y notable importancia del objeto típico sobre el que descansa el bien jurídico y la especial insidiosidad de los focos de peligro emergentes para ambos, dadas sus específicas características y las nuevas modalidades de ataque derivadas de las nuevas tecnologías, permite detectar la necesidad de anticipar la intervención penal.

Así pues, atendiendo a los criterios materiales de desvalor que deben ser tenidos en cuenta a la hora de arbitrar idóneas técnicas de tutela, ni puede esperarse al resultado de daño o perjuicio económico, ni tan siquiera parece posible radicar el desvalor de resultado en la puesta en peligro concreto del bien jurídico.

En la modalidad de apoderamiento, que, **de lege lata**, se halla prevista en el art. 278.1, primer párrafo CP, no se encuentra ningún elemento expreso indicativo de su configuración como delito de peligro concreto o de

peligro hipotético¹³⁰⁵. Sin embargo, ya que la idoneidad de la acción para producir un peligro puede ser inferida merced a una labor interpretativa¹³⁰⁶, conviene ahondar en otros criterios atinentes a la mayor o menor cercanía entre el bien jurídico y la acción para poder desechar la estructura de peligro concreto o verificar la de peligro abstracto o hipotético.

Desde luego, entre el bien jurídico protegido y la acción de apoderamiento del secreto de empresa, no parece que exista necesariamente una **relación de proximidad de lesión**. Como se sabe, en este delito, no se protege la mera situación de reserva o de secreto, interés con el que, sin duda, sí se da una proximidad de lesión, sino que, el bien jurídico tutelado se cifra en el interés económico del empresario. En esta medida, la acción de apoderamiento subrepticio o de mera captación intelectual del sujeto no parece idónea para causar necesaria e inmediatamente la creación de un **concreto peligro de lesión** para el interés económico del empresario, aunque suponga, en cierta forma, la conculcación, potencial o real, de la situación de reserva, en la que descansa --pero en la que no se cifra-- el bien jurídico. De ahí que no pueda afirmarse que el apoderamiento típico del secreto empresarial deba producirse en una situación tal que el bien jurídico haya estado en una situación próxima a la lesión, porque ni necesariamente se produce así en todos los casos, ni es posible ni aconsejable radicar su desvalor de resultado en una puesta en peligro concreto del bien jurídico¹³⁰⁷, ya que supondría

¹³⁰⁵ Por el contrario, otros preceptos ubicados también en el título XIII, contienen expresivos elementos de aptitud, como, por ejemplo, el art. 282 CP («que puedan causar un perjuicio grave y manifiesto a los consumidores...») o el art. 290 CP («de forma idónea para causar un perjuicio económico a la misma, o a alguno de sus socios, o a un tercero»).

¹³⁰⁶ Acerca de las diversas posturas de la doctrina en torno a la necesidad de la presencia en el tipo de elementos normativos expresivos de la potencialidad lesiva, vid. MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte general**, *op. cit.*, p. 111.

¹³⁰⁷ Por el contrario, lo configura como un delito de peligro concreto MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), **Curso de derecho penal económico**, Madrid, 1998, p. 284 y FERNÁNDEZ SÁNCHEZ, M.T., **Protección penal...**, *op. cit.*, pp. 241-242.

demorar la intervención del derecho penal hasta momentos que acaban convirtiéndola en ineficaz¹³⁰⁸.

Sin duda, deviene imposible predeterminedar de antemano el grado de proximidad o de lejanía de la lesión del bien jurídico protegido ante una conducta de apoderamiento. Sin embargo, sí puede constatarse que esta acción encierra una potencial y abstracta peligrosidad de daño para el interés económico del empresario. Así, parece que la estructura de este delito responde a la **del peligro abstracto**, en la medida en que la acción de apoderamiento reviste una peligrosidad inherente o intrínseca para lesionar el bien jurídico y no necesariamente una relación de proximidad¹³⁰⁹.

Esta idoneidad lesiva **en abstracto** se apoya en la previa restricción que se ha hecho ejercido ya en el ámbito del objeto material y en el del propio bien jurídico.

De una parte, el **objeto material** ha sufrido una rigurosa caracterización para poder cobrar relevancia penal y constituirse en elemento típico, asumiendo un contenido material proporcionado por el

¹³⁰⁸ De igual modo, respecto del art. 290, la doctrina ya ha advertido la necesidad de no retrasar la intervención penal hasta momentos o efectos posteriores de efectiva consumación del perjuicio económico, que no siempre son susceptibles de ser constatados cuantitativamente y que, además, la hacen ineficaz (así, vid. TERRADILLOS BASOCO, J., "Los delitos societarios", en DEL ROSAL BLASCO, B. (Ed.), **Estudios sobre el nuevo Código Penal de 1995**, Valencia, 1997, p. 269; VALLE MUÑIZ, J.M., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, op. cit., 1ª. ed., p. 1314 y, posteriormente, VALLE MUÑIZ, J.M./QUINTERO OLIVARES, G./MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, op. cit., 2ª. ed., p. 1335).

¹³⁰⁹ Se muestran partidarios de considerar esta modalidad típica como delito de peligro abstracto BERDUGO GÓMEZ DE LA TORRE, I., "La tutela de la competencia...", en **La reforma penal**, op. cit., pp. 418-419, respecto del art. 276.1 PANCP 1983, aunque al justificarlo parece concebirlo como hipotético; MOLINA BLÁZQUEZ, C., "La criminalización de la competencia desleal...", **PJ**, op. cit., p. 246, respecto del art. 284.1 PCP 1992 y LANDECHO VELASCO, C.M./MOLINA BLÁZQUEZ, C., **Derecho penal español, Parte especial**, Madrid, 1996, p. 252.

criterio de nocividad o dañosidad¹³¹⁰. De esta forma, gracias a la restricción operada en el objeto, que ha sido dotado de contenido material, los secretos de empresa y los objetos en los que se plasma sobre los que recae la acción de apoderamiento serán aquellos capaces de constituir un valioso instrumento competitivo para el empresario y cuya disposición le permita reorganizar su empresa y, en suma, incrementar o mantener su posición competitiva en el mercado.

De otra, el **bien jurídico** ha sido progresivamente delimitado a fin de poder identificar con claridad los intereses merecedores de tutela en el ámbito penal. Así, se ha acudido al derecho de la competencia desleal como criterio para interpretar y dotar de significado propio al bien jurídico-penal. Ello permite, en este momento, desechar cualquier acción típica que no responda a la protección del interés económico del empresario en mantener la reserva de ciertas informaciones, como modo de avance y progreso con base en la propia actividad. Así, con esta secuencial delimitación (y restricción) del bien jurídico a conductas necesariamente provistas de trascendencia concurrencial, se ha desechado la incriminación del apoderamiento que persiga simplemente la tutela de la esfera meramente dominical del empresario. No se protege el derecho subjetivo del empresario frente a otros competidores, sino el recurso a mantener una información, fruto del propio esfuerzo, en secreto, como forma de avanzar en la actividad económica, como estrategia, por tanto, de mantenimiento y consolidación de la posición ganada en el mercado o como forma de incrementar y mejorar la

¹³¹⁰ Como se expuso al abordar el concepto normativo de secreto empresarial, la información relativa al proyecto de pintar las paredes del lavabo de una empresa de color azul, no puede constituir secreto de empresa penalmente relevante, de modo que no será necesario examinar la acción de apoderamiento de dicha información, puesto que no habrá objeto típico. De ahí que el apoderamiento de secretos de empresa carentes de nocividad u ofensividad material, que, por tanto, no son capaces de incidir sobre la competitividad de la empresa, no pueda correr el riesgo de constituir nunca un mero delito de peligro formal, puesto que, en estos casos, la conducta será atípica, por no concurrir uno de los elementos del tipo.

capacidad competitiva. Esto es, con la interpretación del bien jurídico desde el derecho de la competencia desleal, se ha obtenido asimismo un criterio para interpretar el alcance y los límites de estos tipos penales.

Por último, se ha subrayado la aparición de **nuevos focos de peligro** para el bien jurídico derivados del avance tecnológico, que reclaman, con base en **criterios de desvalor material**, la adopción de técnicas de tutela idóneas, lo que ha obligado a identificar con claridad el objeto jurídico de tutela y las fuentes de peligro para el mismo, en atención a su insidiosidad.

En definitiva, se ha acometido una interpretación en clave material de todos los elementos típicos del delito, de modo que este propio contenido puede ahora proyectarse sobre el análisis de la selección de las acciones con potencialidad lesiva.

En otras palabras, la restricción de la responsabilidad se ha ejercido mediante una labor interpretativa sobre diversos elementos típicos, que facilitan, en este momento, la exigencia de que la acción sea positivamente peligrosa. En este sentido, la técnica de tipificación relativa al peligro constituye un paso más en la progresiva afirmación de lesividad y dañosidad material del delito reivindicada ya en otros elementos típicos. Así, difícilmente puede interpretarse la técnica del peligro en un sentido puramente formal, puesto que el resto de elementos han asumido ya un contenido material, que conducirá a interpretar las acciones en clave de peligro necesariamente hipotético, en el que **siempre se generará dañosidad**. En suma, esta restricción de la responsabilidad acotada merced a la labor interpretativa de diversos elementos otorga, pues, una mayor seguridad jurídica, puesto que únicamente cuando la acción coincidente con el tipo sea

peligrosa (aunque sólo potencial o hipotéticamente) para el bien jurídico podrá **sustancialmente** afirmarse la tipicidad¹³¹¹.

Así, parece que la restricción de esos otros elementos hace que se imprima a la acción una **potencialidad de daño intrínseca o constante**, que permite configurarlos como **delitos de peligro hipotético**. No se trata de la consagración legal de una presunción **iuris et de iure** de peligro derivada de un conocimiento estandarizado de la realidad sobre la que se opera, ni ante la exigencia de un peligro concreto para el interés económico del empresario. Si se prefiere, podría decirse que estamos en presencia de un **delito de aptitud intrínseca**, sin que ello suponga exonerar al juez de corroborar en concreto la corrección del pronóstico de peligro, aun inherente, elaborado por el legislador¹³¹². Es decir, el juez deberá constatar la capacidad lesiva de la conducta en el caso concreto objeto de enjuiciamiento, no bastando en este sentido con afirmar el peligro inherente a la acción realizada¹³¹³.

En suma, se trata de una acción con idoneidad lesiva y que, en la medida en que el resto de elementos, en los que se sustenta la estructuración del tipo, ostentan un contenido material, deviene casi una

¹³¹¹ TORÍO LÓPEZ, A., "Los delitos del peligro hipotético...", *op. cit.*, p. 839.

¹³¹² Así ocurre, por el contrario, en los puros delitos de peligro abstracto (así, vid. TERRADILLOS BASOCO, J., *Derecho penal...*, *op. cit.*, p. 51).

¹³¹³ Reclaman también este juicio de corroboración de la potencialidad lesiva en el caso concreto, VALLE MUÑIZ, J.M., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código...*, *op. cit.*, 2ª. ed., p. 1302, respecto del delito de publicidad engañosa, previsto en el art. 282 CP, configurado asimismo como delito de peligro hipotético y TERRADILLOS BASOCO, J., "Los delitos societarios", en DEL ROSAL BLASCO, B. (Ed.), *Estudios sobre el nuevo Código Penal de 1995*, Valencia, 1997, p. 273, respecto del delito societario tipificado en el art. 290, conformado de igual modo como delito de peligro hipotético.

idoneidad **intrínsecamente** peligrosa, pero sin que esa **peligrosidad inherente** suponga la volatilización de la exigencia de ilicitud material¹³¹⁴.

Así pues, puede ya afirmarse que, aunque en el tipo analizado no consta ningún elemento normativo expresivo de la potencialidad lesiva, se ha inferido que dicha potencialidad lesiva se halla implícita en la formulación típica.

En conclusión, pues, un enjuiciamiento teleológico del apoderamiento de secretos de empresa permite reconocer que dicha acción posee idoneidad o aptitud intrínseca para hacer peligrar el objeto de protección, de forma que tutelando el control sobre dicho secreto empresarial se tutela, asimismo, el interés económico del empresario. Aun así, ello no supone la conversión de la acción típica en una mera criminalización de apoderamientos carentes de carga o lesividad potencial para dañar el interés económico, de modo que queda vedado al intérprete entender que el tipo asume un contenido meramente formal, elevando a la categoría de delito, automáticamente, cualquier apoderamiento¹³¹⁵. Se conforma, pues, como un **tipo de peligro hipotético**, entendiendo por tal el que castiga una conducta objetivamente idónea (peligrosa) en una consideración **ex ante** para producir un resultado lesivo¹³¹⁶.

¹³¹⁴ Así, TERRADILLOS BASOCO, J., **Derecho penal...**, *op. cit.*, p. 55, siguiendo a CÓRDOBA RODA, sostiene que no condicionar la pena a la constatación del riesgo supone la «volatilización» de la exigencia de ilicitud material.

¹³¹⁵ Así, vid. respecto del art. 290, TERRADILLOS BASOCO, J., “Los delitos societarios”, en DEL ROSAL BLASCO, B. (Ed.), **Estudios sobre...**, *op. cit.*, p. 273 y VALLE MUÑIZ, J.M., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, *op. cit.*, 1ª. ed., p. 1314 y, posteriormente, VALLE MUÑIZ, J.M./QUINTERO OLIVARES, G./MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, *op. cit.*, 2ª. ed., p. 1335.

¹³¹⁶ Así, TORÍO LÓPEZ, A., “Los delitos del peligro hipotético...”, *op. cit.*, p. 838 y TERRADILLOS BASOCO, J., **Derecho penal...**, *op. cit.*, p. 58.

Por lo que atañe a la **legitimidad político-criminal** de los delitos de peligro, en la medida en que suponen la anticipación de la intervención penal y, por tanto, una considerable ampliación de la punibilidad, reclaman una especial cautela en su empleo.

Como ha señalado unánimemente la doctrina, el principio de intervención mínima y de **ultima ratio** demandan evitar el recurso a los tipos de peligro abstracto en la medida de lo posible, esto es, en aquellos casos en que sea factible la protección del bien jurídico mediante tipos de lesión¹³¹⁷.

En los delitos objeto de análisis, la especial vulnerabilidad del secreto de empresa, sobre el que se sustenta el bien jurídico protegido y los ataques especialmente insidiosos de los que puede ser objeto, hacen que, aunque la acción típica sea potencialmente peligrosa para el bien jurídico, devenga extraordinariamente difícil e inadecuado radicar el desvalor de resultado en un daño o en un riesgo o peligro concreto. Sin embargo, es imprescindible para la salvaguarda del interés económico del empresario el mantenimiento de la reserva. La significación económica del secreto deriva de esa exclusividad fáctica, de forma que el apoderamiento del secreto puede suponer la destrucción o menoscabo del mismo como bien esencialmente económico y posee pues capacidad para poner en peligro el interés económico, aunque entre ellos no exista necesariamente proximidad. Téngase en cuenta, además, la configuración formulada sobre el secreto empresarial, como concreta estrategia competitiva adoptada por su titular por resultar la forma más óptima de aprovechamiento económico de esa información. En este sentido, el empresario puede reorganizar su unidad empresarial en función de esa información de la que dispone, aunque no la

¹³¹⁷ Así, vid., entre otros, TIEDEMANN, K., **Poder económico...**, *op. cit.*, p. 36; TERRADILLOS BASOCO, J., *ibidem* y MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte general, op. cit.**, p. 115.

explote, pero que para él resulta valiosa. De ahí que la exclusividad fáctica del secreto, de la que deriva la mejora competitiva, no sólo se ciña a los beneficios económicos dimanantes de la explotación directa o de la transferencia de una información explotable, sino que, englobe asimismo los que proporciona la ***exclusividad en la propia gestión de dicha información***. Consecuentemente, el contenido del bien jurídico, en cuanto interés económico, no se cifra únicamente en facultades de explotación, sino que comprende asimismo facultades de gestión del secreto y de organización de la propia actividad, que pueden verse directamente menoscabadas en caso de que el apoderamiento ponga en peligro la información secreta de la que se dispone. Por tanto, el menoscabo del bien jurídico se produce también cuando estas facultades se ven amenazadas y, en general, cuando las condiciones de seguridad que son imprescindibles para un disfrute despreocupado de los bienes se ven afectadas¹³¹⁸.

En este sentido, KINDHÄUSER afirma que, en los delitos de peligro abstracto en el ámbito del derecho penal económico, no se sanciona una vulneración actual del bien jurídico (de ahí la estructura de peligro), sino el menoscabo de patrones de seguridad tipificados, cuya eficiencia resulta esencial para el aprovechamiento racional de los bienes¹³¹⁹. De forma que la genuina lesividad del peligro abstracto reside en que un bien sobre el que no

¹³¹⁸ Así, KINDHÄUSER, U.K., “Acerca de la legitimidad de los delitos de peligro abstracto en el ámbito del derecho penal económico”, en ***Hacia un derecho penal económico europeo. Jornadas en honor del Profesor Klaus Tiedemann, op. cit.***, pp. 449. En este sentido, siguiendo a KINDHÄUSER, MARTÍNEZ-BUJÁN PÉREZ, C., ***Derecho penal económico, Parte general, op. cit.***, p. 113, afirma que los delitos de peligro abstracto se conciben como delitos de daño ***sui generis***, es decir, daños autónomos —y no simples fases o estadios previos a las lesiones— que vulneran las condiciones de seguridad imprescindibles para un disfrute de los bienes desprovisto de toda perturbación.

¹³¹⁹ KINDHÄUSER, U.K., “Acerca de la legitimidad...”, en ***Hacia un derecho penal, op. cit.***, pp. 448-449.

puede disponerse de forma despreocupada no es racionalmente aprovechable en su totalidad¹³²⁰.

Sin duda, como ha advertido ya MARTÍNEZ-BUJÁN, la legitimidad de la técnica del peligro abstracto en la protección de bienes jurídicos debe vincularse a ulteriores limitaciones, de modo que dicha tutela será legítima cuando se produzca la vulneración de ámbitos de libertad individual (en nuestro caso, el libre ejercicio de una actividad económica), que se hallen jurídicamente garantizados, es decir, cuya seguridad se inscriba dentro de las competencias del Estado («competencia heterónoma sobre la seguridad»)¹³²¹. De ahí que resulte imprescindible acreditar que la conducta típica puede ser configurada como una **auténtica injerencia en la esfera de libertad ajena jurídicamente garantizada**, lo que, a juicio de MARTÍNEZ-BUJÁN, comporta la necesidad de incorporar al tipo de injusto los elementos denotativos de semejante configuración¹³²².

¹³²⁰ Como ocurre normalmente en el ámbito de los delitos socioeconómicos, el carácter pluriofensivo de ciertas conductas evidencia la doble perspectiva que puede adoptarse en su configuración según el bien jurídico en que se ponga el acento. Así, estos delitos se configuran como delitos de peligro hipotético si se atiende al interés individual del empresario competidor; sin embargo, si se toman en consideración intereses supraindividuales o colectivos, como la competencia por el propio esfuerzo o el fomento del avance y progreso, estos intereses se ven directamente lesionados y no sólo puestos en peligro. De forma que el interés colectivo resulta lesionado al ponerse en peligro hipotético los bienes jurídicos de los individuos concretos (así, destacando esta doble perspectiva, vid. TIEDEMANN, K., *Poder económico...*, *op. cit.*, p. 36; TERRADILLOS BASOCO, J., *Derecho penal...*, *op. cit.*, p. 56-57 y MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte general, op. cit.*, p. 112).

¹³²¹ Así, KINDHÄUSER, U.K., “Acerca de la legitimidad...”, en *Hacia un derecho penal, op. cit.*, p. 449, distingue entre «competencia autónoma» y «competencia heterónoma» sobre la seguridad, entendida ésta como posibilidad de disfrutar sin riesgo de los bienes. La competencia autónoma significa la responsabilidad propia del individuo por sus asuntos. Por contra, la seguridad heterónoma se refiere a la compensación del cuidado que el individuo no puede procurarse, o sólo puede hacerlo con un esfuerzo extraordinario, a la hora de disponer de sus bienes; esta seguridad heterónoma es relevante penalmente cuando está jurídicamente garantizada.

¹³²² MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte general, op. cit.*, p. 114.

Nada impediría, en abstracto, configurar la modalidad de apoderamiento como un delito de peligro concreto o abstracto, puesto que la exigencia de la potencialidad o idoneidad lesiva se hallará implícita en la formulación típica.

Como advierte TERRADILLOS BASOCO¹³²³, a ello debe añadirse la constatación de que la actividad económica y el comercio se desarrolla hoy, mayoritariamente, en el ámbito de grandes empresas¹³²⁴, de modo que las incidencias en el seno de éstas repercuten directa o indirectamente en amplios sectores económicos, lo que evidencia la trascendencia colectiva y la pluralidad de intereses y eventuales bienes jurídicos afectados.

En conclusión, ya que no parece factible otra técnica de tipificación (lesión o peligro concreto) en el arbitrio de la tutela del bien jurídico, dado que se produce la vulneración de la libertad individual de libre empresa garantizada jurídicamente a causa de injerencias indebidas de terceros y puesto que el legislador ha fijado la conducta prohibida con precisión y la prohibición se refiere directamente a un bien jurídico determinado¹³²⁵, **el empleo del peligro hipotético en el art. 278.1, primer párrafo CP parece un recurso lícito y adecuado.**

¹³²³ TERRADILLOS BASOCO, J., “Los delitos societarios”, en DEL ROSAL BLASCO, B. (Ed.), *Estudios sobre...*, *op. cit.*, p. 268.

¹³²⁴ Al respecto, afirma VIDAL VILLA, J.M. *Mundialización. Diez tesis y otros artículos*, Barcelona, 1996, p. 97 (citado en MERCADO PACHECO, P., “El «Estado comercial abierto...», en *Transformaciones del derecho...*, *op. cit.*, p. 128), que, «en la actualidad, se asiste a una *transición* entre la situación anterior en la que predominaba el comercio internacional y la futura en la que existirá únicamente el *comercio interempresarial* a nivel mundial».

¹³²⁵ Así es reclamado en la recomendación número 9 del XIII Congreso Internacional de la Asociación Internacional de Derecho Penal sobre «El concepto y los principios fundamentales del Derecho Penal Económico y de la Empresa», celebrado en El Cairo en 1984 y, en nuestra doctrina, vid., por todos, TERRADILLOS BASOCO, J., *Derecho penal...*, *op. cit.*, p. 56.

Adicionalmente a lo expuesto, la técnica del peligro hipotético evitará los problemas de prueba que suscitaría la corroboración de un resultado de peligro concreto del interés económico, debiendo ser abarcado dicho resultado por el dolo del autor¹³²⁶. Sin embargo, la mayor eficacia que comporta en el ámbito probatorio el uso de la técnica del peligro hipotético no puede admitirse en detrimento de las garantías y con menoscabo del principio de ofensividad, de modo que, según prescribe la recomendación número 9 del XIII Congreso Internacional de la Asociación Internacional de Derecho Penal sobre «El concepto y los principios fundamentales del Derecho Penal Económico y de la Empresa», celebrado en El Cairo en 1984, «la creación de delitos de peligro abstracto no está justificada cuando obedezca exclusivamente al propósito de facilitar la prueba de los delitos»¹³²⁷.

De igual modo, tampoco puede admitirse que la decisión de incriminar o no un delito de peligro hipotético deba «llevarse a cabo, no en base al peligro intrínseco inherente a la acción, sino también al extrínseco que pudiera representar la impunidad de la clase de acciones a que pertenece»¹³²⁸. Desde luego, el principio de culpabilidad y de exclusiva protección de bienes jurídicos determinan que la responsabilidad penal se circunscriba a la valoración del concreto hecho cometido, de modo que, como ya ha manifestado TERRADILLOS BASOCO, no parece convincente un argumento que propone el castigo sobre la base de otros actos peligrosos

¹³²⁶ Así, vid., con carácter general, TIEDEMANN, K., *Poder económico...*, *op. cit.*, p. 36 y, en concreto referido a la acción de revelación de secretos, vid., respecto del art. 277 PANCP, LAMPE, E.J., "La protección jurídico-penal de la competencia...", en *La reforma penal, op. cit.*, pp. 370-371 y, respecto del art. 279 CP, vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 212.

¹³²⁷ Vid., en igual sentido, MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte general, op. cit.*, p. 115.

¹³²⁸ COBO DEL ROSAL, M./VIVES ANTÓN, T.S., *Derecho penal, op. cit.*, p. 328, n. 39 y, de idéntica opinión, siguiendo a estos autores, vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 213.

y no por las características del que se examina¹³²⁹, que o presenta peligrosidad intrínseca o devendrá impune por ausencia de peligro.

1.5. *Iter criminis*.

En materia de *iter criminis*, sostenido que la estructura de la modalidad de apoderamiento, prevista en el art. 278.1 CP, se corresponde con la de un delito de mera actividad, puede admitirse la ejecución imperfecta y, en concreto, el grado de tentativa inacabada¹³³⁰. Téngase en cuenta que ello es posible no sólo en los delitos compuestos de varios actos, sino también en los de **un solo acto**, ya que la tentativa comienza cuando el autor se dispone inmediatamente a realizar el **primer acto típico**¹³³¹. Por el contrario, no cabe tentativa acabada, puesto que, en cuanto se lleva a cabo toda la actividad, ya se ha producido la consumación¹³³².

Por último, debe concluirse el análisis de la primera acción típica, que se halla prevista en el primer inciso del art. 278.1 CP, señalando que las penas contempladas para esta conducta en el art. 278.1 CP, son pena de

¹³²⁹ TERRADILLOS BASOCO, J., *Derecho penal...*, *op. cit.*, p. 54.

¹³³⁰ Admiten formas imperfectas de ejecución MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 75, que, además, considera que, en realidad, el artículo 278.1 CP constituye una «ejecución imperfecta elevada a la categoría de delito independiente»; SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., *Comentarios al...*, *op. cit.*, p. 803; LANDECHO VELASCO, C.M./MOLINA BLÁZQUEZ, C., *Derecho penal español...*, *op. cit.*, p. 252 y SERRANO GÓMEZ, A., *Derecho penal, Parte Especial*, Madrid, 1997, p. 431. En contra, PRATS CANUT, J.M., “Descubrimiento y revelación de secretos...”, en *Delitos relativos a la propiedad...*, *op. cit.*, p. 188.

¹³³¹ Así, vid. LUZÓN PEÑA, D.M., *Curso de derecho penal, Parte general, I*, Madrid, 1996, p. 307.

¹³³² Así, vid. LUZÓN PEÑA, D.M., *Curso de derecho penal, Parte general, op. cit.*, p. 306.

prisión de dos a cuatro años y pena de multa de doce a veinticuatro meses¹³³³.

A continuación, conviene abordar la segunda modalidad típica de acceso ilícito.

2. «Control audiovisual clandestino» y «control ilícito de señales de comunicación».

2.1. Concepto de «interceptación» o «utilización de artificios técnicos de escucha, transmisión, grabación o reproducción».

La segunda de las formas de acceso ilícito a la información, además del apoderamiento, se halla integrada por el control audiovisual clandestino y el control ilícito de señales de comunicación.

La actual acción de acceso al secreto se halla prevista en el código penal en el artículo 278.1, segundo párrafo CP¹³³⁴, que, lejos de incorporar expresamente esta modalidad de ataque, ha optado por reenviar a otro precepto del código (art. 197.1 CP¹³³⁵), que, en sede de delitos contra la intimidad, recoge, asimismo, la interceptación de telecomunicaciones o la

¹³³³ En relación a las diversas consecuencias punitivas que pueden presentar esta acción y otra de las modalidades típicas (revelación) en las distintos grados o fases de ejecución, se suscita una particularidad, cuyo planteamiento y resolución serán abordados al analizar esta última.

¹³³⁴ El art. 278.2 CP castiga al que, para descubrir un secreto de empresa: a) «se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo» o b) **«empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197»**.

¹³³⁵ El segundo pasaje del art. 197.1 CP, al que reenvía el art. 278.1 CP, establece que «el que, para descubrir sus secretos o vulnerar la intimidad de otro, (...), **intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación...**».

utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.

La modalidad de acceso relativa al control auditivo y visual clandestino y al control ilícito de señales de comunicación, prevista según lo indicado por el art. 197.1, segundo párrafo, CP¹³³⁶, comprende no sólo las conductas reconducibles a la idea de control auditivo (grabación, escucha o interceptación de comunicaciones habladas) o visual (filmación-captación de imágenes), sino que se proyecta también sobre conductas de interceptación, grabación o reproducción ilícita de otros medios de comunicación, como las comunicaciones por telefax o a través de una red informática, ya sea de área local (*intranet*) o de área amplia (como, por ejemplo, Internet), indistintamente¹³³⁷.

La incorporación de la tecnología informática al ámbito empresarial y económico y los nuevos atentados que con ello se suscitan asume una incontrovertible trascendencia para el normal desenvolvimiento del tráfico económico¹³³⁸. De ahí que el legislador haya ampliado el ámbito de tutela,

¹³³⁶ Para un análisis exhaustivo de esta conducta, vid., por todos, MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código...*, op. cit., 2ª. ed., pp. 969 y ss.

¹³³⁷ Como se ha expuesto en otro lugar (MORÓN LERMA, E., *Internet y Derecho Penal...*, op. cit., pp. 89 y ss.), una red informática se crea al unir entre sí un conjunto de ordenadores por cualquier medio físico que les permita intercambiar información. Cuando varios ordenadores se unen a través de una red y están en el mismo edificio (sin necesidad de usar telecomunicaciones), se denomina *intranet* o red de área local (LAN- **Local Area Network**). Si para interconectar los ordenadores sí es necesario emplear telecomunicaciones (la red de teléfono), se denomina red de área amplia (WAN- **Wide Area Network**). En una computadora de la red se pueden concentrar los principales archivos. A este ordenador se le conoce como "servidor", y las computadoras que están conectadas al servidor son sus "clientes". El servidor de una red puede conectarse al servidor de cualquier otra red, formándose así redes de redes o inter-redes, cuyo máximo exponente es Internet.

¹³³⁸ Así, vid., por todos, ROMEO CASABONA, C.M., "Delitos informáticos de carácter patrimonial", en *Informática y Derecho*, nº. 9-11, p. 413.

mediante la incorporación de la cláusula abierta de recogida con la que concluye el precepto («o de cualquier otra señal de comunicación...»), al dar cabida típica a las innovaciones tecnológicas en materia de comunicaciones electrónicas o telemáticas¹³³⁹.

En esta medida, con la previsión del apoderamiento de datos del primer inciso del art. 278.1 CP y la modalidad relativa al control ilícito de señales de comunicación, se afronta definitivamente la tipificación del **espionaje empresarial acometido por medios informáticos**, cuyos efectos económicos son de primera magnitud¹³⁴⁰. Según se sabe, las peculiares características de los sistemas informáticos y de su funcionamiento en redes, que los hace especialmente vulnerables a la interceptación, así como la desprotección material y logística de las bases de datos informatizadas, a pesar de las restricciones de acceso (mediante claves) y de lectura de datos (mediante la encriptación o codificación de los datos, ámbito en el que los constantes avances se producen a instancias del propio mercado) facilitan que la información económica valiosa, sometida a tratamiento automatizado, se convierta en una parcela extraordinariamente vulnerable a conductas ilícitas de muy diversa índole¹³⁴¹ (acceso, copia, transmisión, entre otras

¹³³⁹ La introducción de esta cláusula abierta se produjo ya en el art. 497 bis ACP, por mor de la LO 18/1994, al objeto de dar cobertura típica a las comunicaciones inalámbricas, a tenor de la problemática surgida tras el auto de la Audiencia Provincial de Madrid, Secc. 15ª, de 10 de mayo, de 1996, y la posibilidad de que determinadas interceptaciones de señales telefónicas ‘abiertas’ quedasen impunes a la luz del 497 bis ACP. Así, vid., por todos, MORALES PRATS, F., “Servicios de información y espionaje del Estado y secreto de comunicaciones telefónicas (Comentario al auto de la Audiencia Provincial de Madrid, Secc. 15ª, de 10 de mayo de 1996)”, en **AJA**, nº 253, Pamplona, 1996 y MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, op. cit., 2ª. ed., p. 970.

¹³⁴⁰ En este sentido, vid. ROMEO CASABONA, C.M., **Poder informático y seguridad jurídica**, Madrid, 1987, pp. 168 y ss.

¹³⁴¹ Así es advertido, entre otros, por ROMEO CASABONA, C.M., “Delitos informáticos de carácter patrimonial”, en **Informática y Derecho**, nº. 9-11, p. 434 y GUTIÉRREZ FRANCÉS, M.L., “Delincuencia económica e informática en el nuevo Código Penal”, en **Ámbito jurídico de las tecnologías de la información**, Cuadernos de Derecho Judicial, CGPJ, Madrid, 1996, p. 274.

—como, por ejemplo, destrucción, alteración o inutilización de la información—, que, sin embargo, como se expondrá posteriormente, no resultan subsumibles en las conductas ilícitas previstas por el art. 278.1 CP).

Según se ha dicho, esta modalidad de acción resulta proyectable a la interceptación de comunicaciones verificadas en cualquier red informática, ya sea interna de la empresa (intranet), o ya sea externa, como, por ejemplo, en la red Internet, que es la red habitualmente utilizada al ser la que enlaza e interconecta mayor número de ordenadores.

l) En el primer caso (intranet), se puede interceptar, en el sentido de interferencia o intromisión, cualquier comunicación entre los diversos terminales u ordenadores clientes o bien entre uno de éstos y el servidor. Probablemente estas conductas serán acometidas por trabajadores de la propia empresa, que acceden así a la información sin autorización para la ejecución de dicha conducta o con autorización pero no en la forma subrepticia en que se hace.

Así, por ejemplo, X, alumno de un máster en mercados financieros, es contratado en prácticas para desempeñar tareas propias de gestión y análisis de mercados, por una entidad bancaria. X accede informáticamente a otros ordenadores clientes de la red interna y graba ficheros con información confidencial, relativa a documentos elaborados por el propio equipo de análisis de la empresa como soporte de futuras tomas de decisiones, documentos relacionados con valoraciones de inversiones realizadas y un documento con la presentación de una operación bursátil proyectada por dicha empresa y otra del ramo, presentada a los analistas para ser evaluada. Todos estos documentos son reenviados por X a cuentas de correo electrónico suyas abiertas en hotmail.com.

En la determinación de si quien lleva a cabo estas conductas comete espionaje empresarial, deben darse por reproducidas las consideraciones manifestadas en la anterior acción típica y que reclaman un análisis desdoblado. En el caso de que el **acceso** se haya producido **sin autorización**, por ejemplo, vulnerando los **passwords** de las otras máquinas, X comete espionaje empresarial. Por el contrario, si X tenía **autorización** para ejecutar el acceso, al margen de que parezca difícil imaginar que dicha autorización se proyecte a las conductas de reproducción de la información, aun así la presencia del elemento subjetivo cifrado en el ánimo de descubrir, como intención de conocer y no de revelar¹³⁴², sigue suscitando problemas¹³⁴³.

Por el contrario, la conducta podría castigarse como un acto de competencia desleal¹³⁴⁴, como un supuesto de adquisición de secretos por procedimiento indebido, ya que únicamente se requiere que haya sido ejecutada con el ánimo de obtener provecho propio, o de un tercero o de perjudicar al titular del secreto (ex art. 13.2 y 3 LCD).

En conclusión, por lo que se refiere a la conducta de interceptación en una intranet, no existirán problemas para sancionar penalmente conductas de espionaje, salvo en los supuestos de extralimitación, que resultan también problemáticos en el ámbito del apoderamiento¹³⁴⁵.

¹³⁴² Acerca de la doble vía interpretativa del elemento subjetivo del injusto, vid. supra epígrafe relativo al elemento subjetivo.

¹³⁴³ Desde luego, según se ha advertido ya al analizar estos supuestos en el ámbito del apoderamiento, en este momento, se trata de analizar si la conducta descrita merece sanción ya como espionaje o adquisición ilícita del secreto, como primer estadio de una conducta posterior de revelación, difusión, cesión o aprovechamiento del secreto.

¹³⁴⁴ Por supuesto, al margen de otro tipo de responsabilidades de carácter contractual o laboral, cuyo estudio se ha marginado en este trabajo.

¹³⁴⁵ Así se analizará en detalle más adelante, vid. infra epígrafe referente a otras conductas ilícitas asimilables al apoderamiento y, en especial, la conducta de “apoderamiento abusivo”.

II) Asimismo, este precepto resulta proyectable a la interceptación de comunicaciones que se verifiquen en redes telemáticas y, en especial, en Internet. Así, por ejemplo, las que se producen con el empleo de específicos programas rastreadores o programas **sniffers**, que permiten detectar cierta información en la red y cuyo uso facilita el control y lectura de los mensajes que circulan por Internet. Así, estos programas suelen ser utilizados para penetrar en el disco duro de los ordenadores conectados a la red, buscando la información que interesa¹³⁴⁶. Se trata de modalidades de ataque especialmente insidiosas. Suponen un acceso a la información más penetrante, certero y constante, que además pasa inadvertido para la víctima¹³⁴⁷. La subsunción de este tipo de conductas no plantea tampoco mayores problemas, puesto que el art. 278.1 CP, segundo inciso CP —que remite al art. 197.1 CP—define de forma amplia los medios comisivos.

Mayor complejidad suscita la subsunción en ese precepto de algunas conductas ilícitas en la red, cuyo encaje en el vigente código penal no se halla exento de problemas. Así, por ejemplo, las conductas de **hacking** o de mero intrusismo informático, que se hallan desprovistas de cualquier elemento de tendencia subjetiva ulterior y distinto al acceso mismo¹³⁴⁸. El sujeto activo de estas conductas de mero intrusismo informático (**hacker**) conoce a fondo el funcionamiento de los sistemas operativos, de los

¹³⁴⁶ Como se ha expuesto en otro lugar (MORÓN LERMA, E., *Internet y Derecho Penal...*, *op. cit.*, p. 45) el programa «rootkit» (un tipo de **sniffer**) recoge passwords en un fichero de log, tiene una utilidad para borrar registros de log del sistema y modifica los binarios (signos 1 y 0), que permiten detectar la presencia del **sniffer** o su fichero de log.

¹³⁴⁷ Así es destacado por MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código...*, *op. cit.*, 2ª. ed., p. 972, respecto a la vulneración de la intimidad.

¹³⁴⁸ Las conductas de **hacking** pueden definirse como conductas de mero intrusismo informático. Esto es, como comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos y de utilización de los mismos sin autorización o más allá de lo autorizado. Vid., con mayor profusión, MORÓN LERMA, E., *Internet y Derecho Penal...*, *op. cit.*, pp. 41 y ss.

lenguajes de programación y de los protocolos de Internet. La motivación de sus accesos suele radicar en profundizar en ese conocimiento y aprendizaje poniéndose a prueba en una constante superación de retos. Se infiltra subrepticamente en los sistemas para descubrir agujeros o puertas falsas y fallos, demostrar que puede acceder aunque se le impongan barreras lógicas de entrada mediante **passwords** y que, incluso, es capaz de infiltrarse sin dejar huellas, borrando los **logs** necesarios para hacer desaparecer su rastro. Una vez dentro de la máquina el **hacker** ha logrado su propósito.

Es decir, ya que con el acceso no consentido a los sistemas informáticos no se persigue espiar o descubrir secretos de empresa, respecto al encaje en el código penal vigente de estas conductas de mero intrusismo informático, deben distinguirse dos hipótesis. En primer lugar, que estas conductas devengan en resultados ulteriores más graves y que la intrusión haya sido concebida como un medio necesario para conseguir el resultado final (descubrir la intimidad ajena, destruir datos, vulnerar un secreto de empresa, etc.), en cuyo caso la conducta quedará absorbida por estos delitos, como secuencia o estadio típico inicial de los mismos. Y, en segundo lugar, que las conductas no determinen esos resultados o que, aun determinándolos, no hayan sido ejecutadas con ese propósito. En estos supuestos, el encaje se torna conflictivo, debido a los elementos subjetivos del injusto que suelen incorporar tales delitos y, en el caso del art. 278.1 CP, el relativo al ánimo de descubrir un secreto de empresa. Incluso aún manteniendo, como aquí se ha propuesto, una interpretación amplia de este elemento¹³⁴⁹.

En suma, la conducta del **hacker** sólo podrá quedar subsumida en la acción típica analizada en los supuestos en que pueda establecerse,

¹³⁴⁹ Vid. supra epígrafe relativo al elemento subjetivo.

mediante el correspondiente juicio de inferencias, la prueba del elemento subjetivo del injusto, cifrada en la idea de que el **hacker** no obraba tan sólo con un deseo de demostración de pericia técnica, sino también con la finalidad de descubrir un secreto de empresa¹³⁵⁰. Sin duda, en este supuesto, el elemento subjetivo del injusto desempeña una especial función selectiva de las conductas a incriminar. La conveniencia de residenciar lo ilícito en elementos subjetivos deviene una cuestión no exenta de interés ni de complejidad, en la que, sin embargo, no puede profundizarse en este momento. Desde luego, como tortuosa hipótesis de trabajo, podría especularse con la incriminación de estas conductas en el delito de utilización abusiva de equipos terminales de telecomunicación (artículo 256 CP), cuyo principal inconveniente se cifra en la exigencia de la producción de un perjuicio superior a cincuenta mil pesetas, que, naturalmente, no sólo deberá probarse sino que, en sede de tipicidad subjetiva, deberá ser abarcado por el dolo del autor, con lo que se reproducen las objeciones expuestas¹³⁵¹.

Por último, debe señalarse que, como se ha insinuado ya, es posible que la intrusión subrepticia de un **hacker** en un sistema desemboque en una modificación o supresión de datos valiosos para la empresa, en cuyo caso, dada la no previsión de esta modalidad de ataque en los preceptos destinados a regular la vulneración de secretos de empresa, deberá acudir a otros supuestos, abriéndose al respecto dos vías interpretativas. Aunque esta cuestión será abordada posteriormente con detalle, valga anticipar que una de dichas propuestas radica en la aplicación del art. 264.2 CP, regulador de los daños informáticos, aunque al precio de salvar importantes obstáculos

¹³⁵⁰ Así, MORALES PRATS, F./MORÓN LERMA, E., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código...*, op. cit., 2ª. ed., p. 1285.

¹³⁵¹ Acerca de este posible encaje en el art. 256 CP, vid. MORÓN LERMA, E., *Internet y Derecho Penal...*, op. cit., pp. 46 y ss.

como el relativo a la exigencia de producción de un perjuicio económicamente evaluable. Junto a esta propuesta, sin embargo, se sugerirán otras posibles soluciones por las que, específicamente, se optará en este trabajo.

Expuestos escuetamente los problemas que la interpretación de esta modalidad de ataque presenta, estamos en disposición ya de abordar su análisis desde una perspectiva más general.

2.2. Estructura típica.

En cuanto a la **estructura típica** de esta segunda modalidad comisiva, puede afirmarse que ésta únicamente reclama una conducta de control audiovisual clandestino o control ilícito de señales de comunicación, sin necesidad de un ulterior resultado, material o ideal, distinto de la mera interceptación. Ni se requiere el efectivo descubrimiento del secreto (que sólo actuará como elemento de engarce respecto a la modalidad prevista en el artículo 278.2 CP, de difusión, revelación o cesión de los secretos descubiertos), ni ningún proceso de conocimiento o de disponibilidad del secreto en la esfera de un tercero como proceso autónomo de la conducta del autor, ni, en suma, ningún resultado, posterior o simultáneo, consecuencia de la conducta. Se trata, pues, al igual que en la primera modalidad, de un **delito de mera actividad**¹³⁵².

Atendiendo a la especificidad del bien jurídico y a la fragilidad del objeto material, esta figura típica se estructura como un **delito de consumación anticipada**, incorporando al tipo un elemento subjetivo del injusto adicional al dolo y consistente en el ánimo de descubrir un secreto de

¹³⁵² Por el contrario, MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos*, *op. cit.*, p. 128, lo configuran como un delito de resultado.

empresa¹³⁵³. Así, se trata de un **delito mutilado de dos actos**, cuya consumación reclama únicamente la realización de la primera conducta de control ilícito doloso con el ánimo de descubrir un secreto, bastando al efecto la mera constatación de que el agente actúa animado por esta intención. Se adelanta pues el momento de la consumación al acto de interceptación o de empleo de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, sin que se requiera la efectiva toma de conocimiento del secreto de empresa para la perfección típica (así, por ejemplo, la interceptación de una comunicación encriptada, con el empleo de un programa **sniffer**, se consuma en cuanto detecta el e-mail que circula por la red, aunque no pueda descifrarlo). Sin duda, dado el acceso penetrante y certero en la información que estos medios facilitan, comportará normalmente el descubrimiento del secreto empresarial, aunque este descubrimiento siga actuando a modo de elemento de engarce con el tipo agravado de difusión, revelación o cesión del secreto descubierto (art. 278.2 CP)¹³⁵⁴.

Desde la perspectiva de la intensidad de ataque al bien jurídico, deben darse por reproducidas asimismo las consideraciones formuladas respecto de la acción de apoderamiento ya analizada. Se trata de un **delito de peligro hipotético**, ya que la acción posee capacidad potencial para producir un peligro sobre el bien jurídico e, incluso, puede decirse que

¹³⁵³ En este sentido no puede compartirse la definición que proporciona GUTIÉRREZ FRANCÉS, M.L., "Delincuencia económica...", en **Ámbito jurídico...**, *op. cit.*, p. 276, de espionaje informático empresarial o industrial, como la obtención, **con ánimo de lucro** y sin autorización, de los datos almacenados en un fichero informatizado. Sin perjuicio de posibles propuestas en torno a la modificación del elemento subjetivo del injusto, el tipo previsto en el art. 278.1 CP sólo requiere **el ánimo de descubrir un secreto de empresa**, en el que puede subyacer una adicional finalidad que no se reduce, ni debe hacerlo **de lege ferenda**, al ánimo de lucrarse, sino que también puede englobar la de perjudicar a un tercero.

¹³⁵⁴ Así, vid. MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, *op. cit.*, 2ª. ed., p. 970, respecto al descubrimiento de la intimidad.

encierra una **peligrosidad inherente e intrínseca**, que, al igual que en la anterior modalidad, deberá ser verificada en el caso concreto por el juez; se trata de una capacidad potencial de peligro, en una consideración **ex ante**, que reclama su contextualización y corroboración por el juez¹³⁵⁵.

Por último, en materia de **iter criminis**, sostenido que la estructura es la de un delito de mera actividad, puede admitirse la ejecución imperfecta y, en concreto, el grado de tentativa inacabada. Así, por ejemplo, los actos de instalación de artificios técnicos de control clandestino de la imagen o del sonido (colocación de micrófonos o de aparatos de filmación), sin captación efectiva de los mismos, resultan conductas típicas en grado de tentativa inacabada¹³⁵⁶. Por el contrario, no cabe tentativa acabada, puesto que, en cuanto se lleva a cabo toda la actividad, ya se ha producido la consumación.

3. Penalidad.

Las penas previstas para sancionar la última de las formas de acceso ilícito (prisión de dos a cuatro años y multa de doce a veinticuatro meses) son iguales a las de la modalidad anterior, cifrada en el apoderamiento de datos u objetos que se refieran al secreto. Esa equiparación penológica merece ser criticada en la medida en que asimila, desde la perspectiva de las consecuencias jurídicas, modalidades de ataque de distinta insidiosidad. En este sentido, el acceso a los datos por vía informática (art. 278.1, primer inciso, CP) y, sobre todo, el acceso con el empleo de artificios técnicos de

¹³⁵⁵ Por el contrario, lo configura como un delito de peligro concreto, FERNÁNDEZ SÁNCHEZ, M.T., **Protección penal...**, *op. cit.*, pp. 241-242.

¹³⁵⁶ Así, en igual sentido, BAJO FERNÁNDEZ, M./BACIGALUPO, S., *op. cit.*, p. 498. En contra, SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., **Comentarios al...**, *op. cit.*, pp. 803-804, para quien la mera instalación de artificios técnicos no acompañada de su activación o puesta en funcionamiento deviene atípica, pues «consiste en el mero despliegue de una actividad».

control auditivo o visual clandestino o con la interceptación de comunicaciones (art. 278.1, segundo inciso, CP), revelan una insidiosidad mayor que el apoderamiento físico de los soportes u objetos a los que se refiere el secreto o la captación mental o intelectual de la información, por escucha o lectura de la información plasmada en tales objetos. Así pues, conviene formular una breve recapitulación y conclusión crítica respecto a la regulación otorgada por el código a estas dos modalidades de acceso ilícito (apoderamiento e interceptación).

Admitida la insatisfactoria equiparación penológica de modalidades de ataque de desigual gravedad, el primer paso imprescindible para su corrección o subsanación radica en diferenciar los modos de acceso o de obtención del secreto, ***en la medida en que encarnen diferente insidiosidad***. A ello aboca el reconocimiento de que, en la actualidad, los secretos empresariales son almacenados, casi en su totalidad, en equipos informáticos. Al efecto, según se ha puesto de manifiesto¹³⁵⁷, el esclarecimiento del debate en torno a la tutela del bien jurídico frente a los peligros derivados de las nuevas tecnologías reclama partir de ***criterios materiales de desvalor***, que tomen en consideración la afección al bien jurídico, atendiendo, sobre todo, a las fuentes de peligro para el bien jurídico (insidiosidad) y a la especial sensibilidad del mismo.

Esta integración de las nuevas tecnologías en el ámbito empresarial, las extraordinarias ventajas de la gestión electrónica de la información y la implantación generalizada de la telemática ha suscitado una heterogénea diáspora de repercusiones y un gran impacto sociojurídico en todos los países de nuestro entorno europeo y, con especial rigor, en Alemania. En efecto, el legislador alemán no sólo llevó a cabo una profunda reforma

¹³⁵⁷ Vid. supra, capítulo IV, apartado 3.5.

acometida por la 2. WiKG, de 15 de mayo de 1986¹³⁵⁸, sino que ésta vino precedida de un amplio y profundo debate¹³⁵⁹. Así, en respuesta a los nuevos peligros derivados de la criminalidad informática, a las enormes pérdidas económicas sufridas por las empresas alemanas y ante la insuficiencia de la previsión del parágrafo segundo § 17 UWG, ceñido a una escueta y anacrónica sanción del acceso al secreto por conducta «contraria a la ley o a las buenas costumbres», para acoger los nuevos atentados a la información comercial o industrial, el legislador decidió robustecer la protección penal y tipificar el espionaje empresarial y, en concreto, el espionaje informático o electrónico, en el segundo párrafo del § 17 UWG.

Así, en el § 17 UWG, segundo párrafo, se distinguen dos subapartados, de los cuales, por el momento, sólo nos interesa el primero, que prevé lo siguiente:

«Será castigado con la misma pena quien, con finalidad competitiva, en beneficio propio o a favor de un tercero o con la intención de perjudicar al propietario de la empresa,

1. se procura o se asegura sin autorización la obtención de un secreto comercial o industrial a través de:

- a) la utilización de medios técnicos,
- b) la realización de una reproducción material del secreto o

¹³⁵⁸ **Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität**, de 15.5.1986.

¹³⁵⁹ Como ya ha sido señalado en la primera parte del trabajo (vid. supra), las pérdidas materiales que las empresas alemanas sufren mediante el espionaje y la revelación de secretos se contabilizan cada año en más de mil millones de marcos (así, entre muchos otros, vid. DANNECKER, G. "Der Schutz von Geschäfts...", en *Der Betriebs-Berater*, *op. cit.*, p. 1615 y MÖHRENSCHLAGER, M., "Das neue Computerstrafrecht", en *wistra*, 4, 1986, pp. 137 y ss.). Ello motivó la reivindicación de una reforma legislativa que paliase tal situación otorgando una tutela mayor y más fuerte, sobre todo, en el ámbito penal y que, a su vez, afrontase los riesgos derivados de la implantación generalizada de las nuevas tecnologías de la información en el ámbito empresarial. Se reclamaba, en suma, la introducción de nuevos preceptos desde los que emprender la lucha contra la criminalidad informática (así, vid. MÖHRENSCHLAGER, M., *op. ult. cit.*, pp. 128 y ss.).

- c) la sustracción o el apoderamiento de una cosa en la que se halle incorporado el secreto»¹³⁶⁰.

En este precepto, que merece una valoración positiva, se separan adecuadamente los diferentes modos de asegurarse o procurarse el secreto, atendiendo a la diferente insidiosidad de los mismos. Así, se regula en el apartado tercero [letra c)], la sustracción subrepticia del soporte y se destinan las otras dos previsiones a las conductas derivadas de la utilización de medios técnicos, que, en la mayoría de los casos, serán medios informáticos [letras a) y b)]. Sin duda, el legislador alemán podría haber perfilado más estas previsiones, aislando las conductas propiamente derivadas de abusos informáticos y estratificando las penas consecuentemente, pero aun así, resulta una regulación avanzada que permite solventar diversos aspectos problemáticos que, por ejemplo, en el código penal español no encuentran un encaje pacífico, como se tendrá ocasión de exponer¹³⁶¹.

En buena lógica, pues, debe concluirse que lo deseable sería distinguir, entre los distintos modos de acceso o de obtención indebida de los secretos, las conductas de **apoderamiento subrepticio de soportes** u objetos que se refieran al secreto y de captación intelectual del mismo --que no sea fruto de un abuso informático-- y las **conductas de acceso ilícito** a la información, mediante la utilización de las nuevas tecnologías de la información. Asimismo, esta distinción debería llevar aparejada la correspondiente estratificación punitiva, instituyendo las penalidades más graves para aquellos supuestos en los que el sujeto emplea medios más

¹³⁶⁰ § 17, II, 1 UWG.

¹³⁶¹ Vid. infra, epígrafe destinado a otras conductas ilícitas.

insidiosos y certeros para acceder al secreto de empresa y, por tanto, más peligrosos para el interés económico del empresario¹³⁶².

A nuestro parecer, la conducta de apoderamiento, en cuanto modalidad básica de atentado al secreto de empresa, debe ser asimilada –por lo que se refiere a su previsión como acción atentatoria y, por tanto, sin perjuicio de los matices anteriormente formulados--, a la conducta de interceptación, como correctamente hace el código. Sin embargo, esas dos modalidades no toman en consideración algunas otras que, desde la perspectiva del bien jurídico, presentan idéntica carga lesiva. En concreto, me voy a referir a la conducta de reproducción, a la de apoderamiento cometido con abuso de funciones o con extralimitación y, por tanto, “apoderamiento” abusivo y a la destrucción, alteración o inutilización de los datos que componen el secreto.

III. Otras conductas ilícitas: la reproducción, el “apoderamiento” abusivo y la destrucción, alteración e inutilización.

Frente a las conductas analizadas (apoderamiento e interceptación), que, aun con los problemas indicados, de modo expreso aparecen recogidas en el código, no se prevén, en los artículos 278 a 280 CP, otras modalidades de ataque, que pueden, de igual forma, incidir sobre el secreto de empresa, como son, por ejemplo, la reproducción, el “apoderamiento” abusivo y la destrucción, alteración o inutilización del secreto.

Efectivamente, según se comprobará, la regulación de los secretos empresariales frente a agresiones o abusos informáticos en el vigente código penal español adolece de sistemática. No se ha acometido desde un

¹³⁶² Así es advertido por MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código...*, *op. cit.*, 2ª. ed., p. 972, en el ámbito de los delitos contra la intimidad.

planteamiento articulado del bien jurídico protegido, en el que se afronte de modo integral su tutela frente a los peligros derivados de esta implantación generalizada de informática, rasgo que ha presidido la reforma en este extremo¹³⁶³. De ahí la necesidad de plantear sucintamente la reflexión en torno a estas conductas, que se hallan estrechamente vinculadas a los abusos informáticos.

La importancia que la información reviste actualmente para el desarrollo económico y social no tiene parangón con la que ha podido tener en cualquier otro periodo histórico¹³⁶⁴. Lógicamente, para las empresas, cuyo desenvolvimiento, organización, capacidad competitiva y posición en el mercado se sustenta en la disposición de informaciones valiosas económicamente, este proceso se ha agudizado. Si a ello se añaden las repercusiones de las nuevas tecnologías, que han posibilitado mayor volumen de información y mayor facilidad de acceso, la seguridad de este flujo constante de información se conforma como una cuestión de crucial importancia para el mantenimiento de su nivel de desarrollo y progreso y, también, para el de la entera colectividad. Constatado el relieve que ostenta la información en el actual marco socioeconómico y la trascendencia, por tanto, que su seguridad asume, deben analizarse ya los problemas que se plantean desde la perspectiva penal.

Y, desde este punto de vista, el estudio se centrará en examinar la protección arbitrada sobre la **información empresarial sensible, almacenada, procesada y transmitida mediante equipos informáticos frente a posibles**

¹³⁶³ Así, vid. GUTIÉRREZ FRANCÉS, M.L., “Delincuencia económica...”, en *Ámbito jurídico...*, *op. cit.*, p. 297.

¹³⁶⁴ Así es destacado por numerosa doctrina; vid., por todos, RIBAGORDA GARNACHO, A., “Seguridad de las tecnologías de la información”, en *Ámbito jurídico de las tecnologías de la información*, CDJ, CGPJ, 1996, p. 309 y DEL PESO NAVARRO, E., “La seguridad de la información”, en *AIA*, nº 26, 1998, p.1.

ataques cometidos abusando de estas modernas técnicas. Aunque, generalmente, como posibles objetos de la criminalidad informática se suele hacer referencia al **hardware**, para aludir al propio ordenador, al **software** y a los datos, en nuestro caso, sólo se abordará la información o datos valiosos económicamente, en cuanto **objeto del secreto de empresa**, teniendo en cuenta que uno de estos objetos, en concreto del denominado secreto industrial, es precisamente el **software** o programas de ordenador¹³⁶⁵.

Como se sabe, la posibilidad de comprimir los datos en un espacio mínimo ha suscitado nuevas vías de puesta en peligro de los mismos, favorecidas por el **rápido acceso** técnico sobre ellos --desde el propio ordenador que los almacena o a distancia por vía telemática-- y por las **modernas técnicas de copiado**¹³⁶⁶. A tenor de este foco de riesgos, emerge como objetivo indispensable garantizar la seguridad de la información contenida en redes, soportes o sistemas informáticos, sobre cuya reserva se sustenta el secreto de empresa como bien económico.

Al objeto de esclarecer estas nuevas fuentes de peligro para el bien jurídico, y dada la trascendencia que asume en la delimitación de las acciones típicas, conviene determinar cuáles son las características peculiares o diferenciables de la información contenida en soportes, sistemas o redes informáticas, de la información contenida, por ejemplo, en un documento o soporte analógico, que deben ser preservadas, para una adecuada salvaguarda del secreto¹³⁶⁷.

¹³⁶⁵ Vid. supra, capítulo II, epígrafe relativo al software como objeto del secreto industrial.

¹³⁶⁶ Vid., en igual sentido, MÖHRENSCHLAGER, M., "Das neue Computerstrafrecht", en *wistra*, *op. cit.*, p. 137.

¹³⁶⁷ Ello debe interpretarse en el bien entendido que las características esenciales de la información se predicán independientemente de la naturaleza del soporte que la contiene. Ahora bien, las peculiaridades de los sistemas informáticos obligan a pormenorizar el análisis de estos caracteres, a fin de detectar las múltiples fuentes de peligro que se

En la actualidad, se entiende por seguridad de la información el mantenimiento de la confidencialidad, integridad y disponibilidad de aquélla¹³⁶⁸. Así, la **confidencialidad** reclama que la información sea revelada exclusivamente a los usuarios autorizados, en la forma y tiempo determinados; la **integridad** exige que la información sea modificada (incluyendo su creación y borrado) sólo por personal autorizado; y, por último, la **disponibilidad** demanda que la información sea utilizable en el momento y del modo en que lo requieran los usuarios autorizados¹³⁶⁹.

Por tanto, cualquier acción capaz de provocar una pérdida o daño en la confidencialidad, integridad o disponibilidad de los datos, constituye una amenaza de la seguridad de la información y, en esa medida, una conducta idónea para generar un riesgo sobre el mantenimiento del secreto de empresa como bien esencialmente económico y, por tanto, una conducta con **capacidad de afección del bien jurídico** protegido.

Estas amenazas pueden cifrarse en comportamientos que atenten contra una de dichas características o contra varias de ellas. Así, suponen una amenaza de la **confidencialidad** de los datos, las conductas de acceso

suscitan y, posteriormente, delimitar correctamente las acciones típicas expresamente contempladas e identificar las que se hallan todavía ayunas de previsión. Así, por ejemplo, la comunicación oralmente o la grabación en una cinta de casete de la mezcla exacta de los ingredientes de la coca-cola no parece susceptible de alteración; si se contiene en un documento de papel o grabada, por ejemplo, en una cinta de vídeo, será difícilmente alterable y, probablemente, si se lleva a cabo la supresión de algún fragmento será detectado con facilidad; por el contrario, si esa misma información se halla almacenada en soporte informático resultará fácilmente modificable y, además, la alteración podrá pasar desapercibida para la víctima. Todo ello evidencia la necesidad de perfilar los ataques que puede sufrir la información contenida en soporte informático o en la red.

¹³⁶⁸ Así, vid. RIBAGORDA GARNACHO, A., "Seguridad de las tecnologías de la información", en *Ámbito jurídico...*, *op. cit.*, p. 312.

¹³⁶⁹ Así, vid. RIBAGORDA GARNACHO, A., "Seguridad de las...", en *Ámbito jurídico...*, *op. cit.*, p. 312-313 y DEL PESO NAVARRO, E., "La seguridad de la información", en *AIA*, nº 26, 1998, pp. 2-3.

inconsentido a la información o de reproducción de la misma; entre las que suponen un riesgo sobre la **integridad** de los datos, se hallan la introducción de algún dato, la alteración, la ocultación, la supresión o borrado y, también, la creación de duplicaciones; por último, atenta contra la **disponibilidad** de la información la inutilización de la misma, mediante su encriptación o codificación o, por ejemplo, mediante la inserción de alguna subrutina o bomba lógica de actuación retardada. Así, por ejemplo, el caso de un empleado que programa la inutilización o, incluso, la destrucción de algunos ficheros, para el supuesto en que su nombre desaparezca de la lista de empleados de la empresa¹³⁷⁰.

Pues bien, algunas de estas modalidades atentatorias no se hallan específicamente contempladas en el código, aun cuando poseen una carga lesiva análoga a la del apoderamiento o de la interceptación. Así ocurre, por ejemplo, con la conducta de **reproducción ilícita de la información**, a cuyo análisis se procede.

1) La reproducción.

La primera de las acciones ayuna de referencia legal está integrada por la conducta de reproducción. Este comportamiento abarca, esencialmente, el cometido con el empleo de medios técnicos y, en especial, la copia de la información realizada por medios informáticos, cuyas

¹³⁷⁰ Esta modalidad de destrucción o de sabotaje informático se denomina «**time bombs**» o bomba lógica de actuación retardada. En estos casos, la destrucción de los ficheros se produce, tras un lapso de tiempo, en virtud de indicaciones precisas como la presencia o ausencia de un dato, que puede ser una hora, un código o un nombre (así, vid., entre otros, CORCOY, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en MIR PUIG, S. (Comp.), **Delincuencia informática**, Barcelona, 1992, p. 151; ROMEO CASABONA, C.M., "Los delitos de daños en el ámbito informático", en **CPC**, nº 43, 1991, pp. 95-96 y GONZÁLEZ RUS, J.J., "Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos", en **Jornadas sobre delincuencia informática, Estudios jurídicos del Ministerio Fiscal**, III, Madrid, 1997, p. 526).

características los dotan de una especial peligrosidad. Así, por ejemplo, el supuesto en que no sólo se produce el apoderamiento de un documento contenido en cualquiera de las memorias electrónicas del ordenador, sino también la posterior **reproducción ilícita del mismo en un disquete por el sujeto a fin de procurarse certeramente el contenido de la información**¹³⁷¹.

Sin duda, como se ha sostenido, el apoderamiento no puede ser interpretado en una reconducción conceptual al esquema clásico de los delitos patrimoniales, sino que reclama una especificidad hermenéutica que lo configura como un apoderamiento intelectual. Y, en esta medida, analizar si la acción de reproducción asume entidad propia o, por el contrario, queda ya absorbida por la de la conducta de apoderamiento, no es tarea sencilla. Al respecto, diversos criterios deben ser tenidos en cuenta.

De una parte, la información económica generalmente resulta compleja, lo que en ocasiones se vincula al mayor esfuerzo que su obtención requiere¹³⁷². Es decir, no se trata, como puede ocurrir, pongamos por caso, en los delitos contra la intimidad, de datos sencillos o aislados, cuya mera visión permite su memorización o retención intelectual --y, en esa medida, el deslinde conceptual o lesivo entre acceso y reproducción puede resultar más complejo--. Esto es, por ejemplo, si se visiona en pantalla el nombre y apellidos de una persona que tiene SIDA o que es homosexual, será innecesario grabar dicha información para poder hacer un uso posterior de la misma. Ahora bien, si se visiona en pantalla un procedimiento de montaje de una nueva serie de coches, la fórmula de un nuevo producto

¹³⁷¹ Así, los supuestos en que el sujeto visiona en pantalla la información y la copia para tener una fidedigna reproducción de la misma, o bien aquellos casos en los que el sujeto, sin visionar la información, como sabe dónde está, la copia directamente.

¹³⁷² Pensemos, por ejemplo, en los programas informáticos o en la obtención de nuevas formas de energía.

adelgazante, o un listado de clientes con un pequeño historial de cada uno, en el que conste su antigüedad, hábitos de compra, preferencias, descuentos que se le practican, entre otras informaciones, será imposible asegurar su obtención si no se hace una copia de la misma.

De otro lado, la posibilidad de comprimir datos en un espacio mínimo ha suscitado nuevas fuentes de peligro para los mismos, que se han visto incrementadas no sólo por el rápido acceso técnico sobre ellos sino especialmente por las **modernas técnicas de copiado**. Si el sujeto activo hubiese tenido que reproducir con medios analógicos --en vez de digitales-- la información, es muy probable que ni hubiese sido posible ni hubiese pasado inadvertido. En esa medida, desde el momento en que se recurre a estas técnicas, el medio comisivo revela una mayor insidiosidad que el mero apoderamiento intelectual de los datos.

Así pues, teniendo presentes estos criterios, a nuestro juicio, la complejidad de la información económica junto con las modernas técnicas de copiado, que potencian su vulnerabilidad o sensibilidad, han hecho que, concretamente en el ámbito de los delitos relativos a la protección del secreto de empresa, **la conducta de reproducción ilícita de la información se conforme quizá con un entidad y un desvalor autónomos e independientes** de la conducta de apoderamiento anteriormente analizada.

En este sentido, quizá uno de los escurridizos criterios de discernimiento entre el apoderamiento intelectual y la reproducción de la información pueda radicar en la memorización o retención intelectual. Esto es, uno de los parámetros integradores del ámbito típico del apoderamiento de los datos vendría suministrado por la posibilidad de memorización, es decir, por la posibilidad de que el secreto pueda ser retenido intelectualmente. De este modo, la información, que, por su cantidad o su

complejidad, no pueda ser memorizada, con arreglo a un baremo estándar, podrá ser objeto de diversas modalidades de ataque para lograr su aseguramiento, ya sea mediante su apoderamiento o ya sea a través de su reproducción. Así, este criterio podría erigirse en un indicador de la gravedad de la modalidad de ataque, en la medida en que, en algunos casos, la memorización podrá agotar ciertos ataques contra la integridad de la información contenida en redes, soportes o sistemas informáticos y, en otros casos, no, ya que será necesario copiar la información para asegurarse su contenido y un posible uso posterior de la misma. En otras palabras, si el secreto puede ser retenido por mera lectura, quizá se trate de una información de menor complejidad, cuyo aseguramiento puede producirse mediante su propia captación intelectual. Y, por el contrario, si para su disposición se requiere una copia, el secreto probablemente se compondrá de una información más compleja, que quizá haya reclamado un notable esfuerzo y cuyo aseguramiento implica, en este caso, una mayor insidiosidad.

Admitido lo anterior, esto es, la relevancia que puede ostentar ***per se*** la conducta de reproducción, procede ya examinar cómo se regula en el código la punibilidad de esta conducta.

El código no contempla la conducta de reproducción como modalidad de ataque independiente. Únicamente aparece parcialmente contemplada en la modalidad de interceptación, en cuya regulación el código sanciona tal acción y cualquier reproducción posterior (control ilícito de señales de comunicación, ex art. 278.1, segundo párrafo y 197.1, segundo párrafo CP). Así, esta laguna podría cubrirse subsumiendo la conducta en esta segunda secuencia o modalidad típica relativa al control ilícito, cuando la reproducción siga a una previa interceptación.

Ahora bien, dicha solución no será posible si se trata de una conducta de **reproducción** acometida desde una máquina, sin interferencia o intromisión en ninguna red de comunicación. En este supuesto, ya que no se prevé una referencia expresa y dada la limitación formulada, debe examinarse si podrá quedar incluida en la primera modalidad analizada, relativa al apoderamiento, prevista en el art. 278.1, primer párrafo CP.

Desde una perspectiva valorativa y de afección al bien jurídico, se constata que no se trata sólo de un apoderamiento o acceso a los datos sino de un acceso inicial y una **ulterior reproducción subrepticia**. Esto es, probablemente, en estos casos, se emplea un dispositivo técnico de entrada y salida (el disquete) que permite al sujeto reproducir, en un soporte pequeño y en un lapso de tiempo insignificante, una extraordinaria cantidad de información, concentrada en un espacio reducido. Es decir, no se trata sólo de un acceso a la información penetrante y certero, sino de un **aseguramiento del secreto para un posible uso posterior del mismo**, mediante la realización de una copia, que además pasará inadvertida para la víctima.

Desde luego, a pesar de que la conducta enjuiciada no se encuentra tipificada --análogamente a como se ha hecho en la interceptación-- en la modalidad de apoderamiento, prevista en el art. 278.1 CP, lo cierto es que podrá integrarse en su ámbito de tutela, en la medida en que la conducta de reproducción siempre implicará una conducta previa de acceso, independientemente de que se haya descubierto o no efectivamente el secreto¹³⁷³. Aunque, sin duda, **el apoderamiento puede constituir un medio comisivo menos grave** que la reproducción ilícita de la información.

¹³⁷³ Como se sabe, el conocimiento del secreto no es un requisito típico, sino tan sólo un elemento de engarce con la siguiente secuencia típica de difusión, revelación o cesión del secreto. Así pues, resulta irrelevante para la consumación del acceso ilícito o reproducción ilícita que el sujeto haga una copia del secreto, sin llegar a conocer su contenido, para entregárselo posteriormente a un tercero.

Así pues, puesto que se trata de acciones diversas, **de lege ferenda**, la modalidad de ataque relativa a la reproducción debería asumir relevancia y autonomía penal, tanto si la lleva a cabo un sujeto no autorizado para acceder al secreto y, por tanto, hay un acceso ilícito, en cuyo caso la reproducción puede ser un plus y, por ello, no debe quedar impune, como en los casos en que no hay tal acceso ilícito, ya que no hay previo apoderamiento o simplemente se copia porque se está autorizado para ello, aunque no para los fines con que se hace¹³⁷⁴.

En buena lógica, pues, el legislador debería hallar una fórmula que permitiese aprehender la diferente gravedad que puede suponer la conducta de acceso y la de reproducción, como modo de aseguramiento del secreto. Algo parecido a lo que ha hecho al regular la infidelidad en la custodia de documentos y la violación de secretos, en el ámbito de los delitos contra la Administración Pública, en los que se distingue entre la información documental (arts. 413 a 416 CP) y la información no documental (arts. 417 y 418 CP). Sin embargo, como se ha sugerido ya anteriormente, el apoderamiento de datos, documentos o soportes referidos al secreto, sancionado en el art. 278.1 CP, parece arbitrarse únicamente sobre la tutela de **secretos documentales** o de soporte análogo.

De ahí que sería conveniente o bien distinguir entre estas diferentes modalidades de ataque o bien emplear un verbo que permita aprehender ambas, como podría ser la previsión del «aseguramiento sin autorización del

¹³⁷⁴ No se nos oculta que esta disociación de las acciones de acceso y reproducción quizá no se produzca siempre, de modo que en algunos casos baste el apoderamiento para aprehender el total desvalor de la conducta. Ahora bien, en nada estorba la previsión de la conducta de reproducción, puesto para esos supuestos más tradicionales será suficiente el apoderamiento, pero para los otros devendrá necesaria la reproducción, para agotar la conducta ilícita.

secreto», como se contiene en el § 17, II, 1 de la ley de competencia desleal alemana (UWG).

Además, el ordenamiento alemán [§ 17, II, 1, letra b) UWG] contempla, específicamente, esta agresión a la integridad de la información o del secreto (en especial, el contenido en soportes, sistemas o redes informáticas), al prever el castigo de la **producción o realización de una reproducción material del secreto**¹³⁷⁵, en la que tienen cabida las copias obtenidas mediante el proceso electrónico o la transmisión a otro soporte de datos o de software¹³⁷⁶.

En conclusión, pues, respecto de la previsión en exclusiva de la acción de apoderamiento, convendría contemplar de forma separada la acción de reproducción ilícita del secreto. El específico desvalor que asume –dada la especial complejidad del objeto y la gravedad de la conducta– respecto del apoderamiento aconsejaría la incorporación específica de esta modalidad. Desde luego, sería preferible incluir la reproducción del secreto por medios informáticos en la esfera de supuestos caracterizados por su mayor insidiosidad. Por tanto, si se reservase un ámbito típico (por ejemplo, en el vigente código, el del apartado primero del art. 278.1 CP) al apoderamiento subrepticio, la reproducción debería preverse junto a los atentados fruto de los abusos técnicos o informáticos.

Y esta ausencia de previsión legal se halla estrechamente vinculada con el siguiente ámbito de conflicto que es el relativo a las extralimitaciones,

¹³⁷⁵ «Será castigado con la misma pena quien, con finalidad competitiva, en beneficio propio o a favor de un tercero o con la intención de perjudicar al propietario de la empresa, 1. se procura o se asegura sin autorización la obtención de un secreto comercial o industrial a través de: a) la utilización de medios técnicos, b) la realización de una reproducción material del secreto o c) la sustracción o el apoderamiento de una cosa en la que se halle incorporado el secreto».

¹³⁷⁶ MÖHRENSCHLAGER, M., “Das neue Computerstrafrecht”, en *wistra*, *op. cit.*, p. 138.

de modo que si se previese la reproducción, en gran parte, también se solventaría el problema del “apoderamiento” abusivo.

II) El “apoderamiento” abusivo.

La segunda de las acciones vinculada o asimilable al apoderamiento, se integra por el acometido con autorización para acceder a los datos o adueñarse de los soportes, pero abusando de dicha autorización --o sea, no en la forma en que debiera hacerlo, sino dándole un uso distinto--.

Esta modalidad de ataque reconducible al abuso de funciones o a la extralimitación, no se halla prevista ni en el ámbito del apoderamiento ni en el de la interceptación. Y el problema básico que se suscita al intentar subsumir esta acción en la modalidad típica del apoderamiento, radica en que en ésta el apoderamiento es siempre ilícito y, en estos supuestos, hay una previa situación lícita.

Así, por ejemplo, el supuesto en que uno de los trabajadores del departamento de marketing de una empresa, con autorización para acceder a las nuevas estrategias publicitarias o de captación de nuevos clientes, sustrae el **software** en el que se contiene una nueva fórmula de descuento para las agencias de viajes clientes de la empresa, con el fin de divulgarlo o explotarlo posteriormente. Esto es, el sujeto con autorización para acceder a la información (situación lícita, por tanto) se garantiza un conocimiento seguro o duradero del secreto, pero mediante la **sustracción (o realización) --ahora ya-- no autorizada** de una copia de la información o, como mínimo, no autorizada para los fines con que pretende utilizarla. En esta medida, cabe plantearse si se apodera --o, si se prefiere, si se asegura-- el conocimiento **indebidamente**.

Pues bien, no se halla exento de problemas un posible encaje de estos actos en la modalidad básica de apoderamiento, tal como se haya configurada, **de lege lata**, en el vigente código penal (art. 278.1 CP). Esta conducta descansa sobre el mero apoderamiento del secreto sin poner el acento en el presupuesto que debería presidir la elaboración e interpretación de todas las normas destinadas a la regulación de los secretos empresariales, asentando la ilicitud de la conducta en que no resulte fruto del propio esfuerzo.

Dado que con la previsión de estas figuras no se instituye un mecanismo de protección de derechos o posiciones jurídicas subjetivas, que permitan a su titular excluir a cualquier tercero del contacto con los secretos, las conductas que se tipifican **no son concurrentialmente reprochables en sí mismas**, sino por las circunstancias en que tienen lugar¹³⁷⁷. Y, a los efectos que aquí interesan, la **adquisición ilícita** del secreto será la que suponga una acto de apropiación indebida del mismo y del esfuerzo ajeno.

Pues bien, esta idea básica es la que debe informar las modalidades típicas que se incriminen y, entre ellas, el acceso al secreto. Al efecto, diversas soluciones, de ámbito nacional y de derecho comparado, parecen sugerentes, entre las que pueden destacarse dos.

Empezando por el derecho español, es conveniente examinar la configuración y alcance de la violación de secretos en la normativa sectorial de carácter civil. Así, el artículo 13.2 LCD establece que «Tendrán asimismo la consideración de desleal la adquisición de secretos por medio de

¹³⁷⁷ En igual sentido, vid. MASSAGUER FUENTES, J.J., *Comentario a la ley...*, *op. cit.*, p. 393.

espionaje o procedimiento análogo»¹³⁷⁸. Esto es, se declara que **sólo** serán desleales **ciertas adquisiciones**. Y, en este contexto, las fórmulas enumeradas --adquisición por medio de espionaje o procedimiento análogo—constituyen actos de apropiación de los soportes o de toma de conocimiento de la información, que resultarán **indebidos** si quien los realiza no guarda una relación con el titular que le autorice a su ejecución o que le autorice en la forma en que se hace¹³⁷⁹.

Análogamente, en el marco del derecho comparado, el legislador alemán proporciona también una adecuada pauta de regulación, al tipificar la sanción del que «1. **se procura o se asegura sin autorización** la obtención de un secreto comercial o industrial a través de: a) la utilización de medios técnicos, b) la realización de una reproducción material del secreto o c) la sustracción o el apoderamiento de una cosa en la que se halle incorporado el secreto»¹³⁸⁰.

Con esta fórmula se puede lograr una adecuada delimitación, entendiendo que actúa «sin autorización» el que se procura o asegura el acceso a informaciones empresariales mediante una actividad dirigida a ello contra la voluntad expresa o presunta del titular del secreto o bien obteniendo su aquiescencia mediante el engaño, esto es, no quien obtiene dicho acceso casualmente¹³⁸¹.

¹³⁷⁸ Como se observa, el ámbito de las conductas previstas en relación a la toma de conocimiento ilícita del secreto es el mismo en la normativa penal y en la civil, cuya regulación, pues, en este aspecto, se solapa.

¹³⁷⁹ Así, vid. MASSAGUER FUENTES, J.J., **Comentario a la ley...**, *op. cit.*, p. 401.

¹³⁸⁰ § 17, II, UWG.

¹³⁸¹ Exposición de Motivos del anterior Proyecto gubernamental anterior a la reforma de la UWG (consultado en MÖHRENSCHLAGER, M., "Das neue Computerstrafrecht", en **wistra**, *op. cit.*, p. 139).

Así pues, **de lege ferenda**, sería conveniente modificar la configuración típica del apoderamiento, de forma que se aprehenda la condición de intangibilidad característica del secreto empresarial así como el contenido material del injusto que caracteriza estos delitos, en el sentido expuesto. Tal conclusión se alcanza desde el entendimiento de que no sólo son accesos ilícitos los apoderamientos subrepticios o sin autorización, sino también aquellos que se cometen accediendo al secreto con autorización, pero no en la forma en que debiera hacerlo, sino dándole un uso distinto y, por ello, con extralimitación o con abuso de funciones. Ello determina que lleva a cabo un acceso ilícito quien se procura o asegura el secreto **de forma indebida o abusiva**.

A tal efecto de reforma, puede sugerirse la incorporación de algún otro verbo --como los términos **adquirir** (empleado por la LCD), **procurarse**, **asegurarse**, **obtener** (acuñado en el art. 273 PCP 1994) e incluso **acceder**, aunque este último parece más idóneo para designar la toma de conocimiento de la información registrada en soporte informático-- junto con/o la introducción de la cláusula **sin autorización**.

En suma, una configuración típica destinada a castigar a quien adquiera, aprehenda, se procure, se asegure u obtenga ilícitamente la información, ya sea por apoderamiento subrepticio, por sustracción o reproducción de la misma, etc., teniendo presente que lo relevante es **la adquisición o el aseguramiento indebidos o abusivos, acometidos contraviniendo las reglas, esto es, fuera de los cauces legalmente establecidos**.

En conclusión, estas dos modalidades ayunas de referencia legal (reproducción y “apoderamiento” abusivo), deben ser asimiladas al apoderamiento, como modalidad de ataque básica, en la que puede

plantearse, aunque con serios obstáculos, su encaje **de lege lata**, ya que, a nuestro parecer, encarnan, asimismo, supuestos de accesos ilícitos o indebidos.

A continuación, procede analizar la tercera modalidad de ataque desprovista de previsión específica en estos delitos, que, sin embargo, presenta unos perfiles distintos de las dos anteriores y que, por tanto, no será asimilable al apoderamiento, sino que reclamará otro contexto o ámbito de resolución jurídica.

III) La destrucción, alteración o inutilización.

La destrucción, alteración o inutilización del secreto empresarial constituye la tercera de las modalidades de ataque, que, estrechamente vinculadas a comportamientos fruto de abusos informáticos, se hallan ayunas de previsión específica en la regulación de los secretos. Así, en su estudio será indispensable, en primer lugar, averiguar si estas conductas de destrucción, alteración, inutilización y otros daños o deterioros, son capaces de incidir sobre el objeto material del delito y sobre el bien jurídico; a continuación, deberá examinarse cuáles son las vías instauradas en el código penal vigente para sancionar tales acciones y, por último, a tenor de las conclusiones de derecho positivo obtenidas, será oportuno reflexionar acerca de la conveniencia de formular una propuesta de reforma legislativa.

I) Para averiguar si se trata de acciones con capacidad ofensiva, conviene, en primer lugar, proceder a una breve definición de las mismas. Así, la conducta de **destrucción** implica la supresión o borrado total de los datos, la **alteración** se integra por comportamientos de inserción de datos,

modificación, supresión parcial, la **inutilización** puede llevarse a cabo mediante la ocultación o la encriptación¹³⁸².

Estas conductas, además, pueden asumir especial lesividad si el secreto de empresa se cifra en un programa de ordenador (así, por ejemplo, el software de control de producción o de gestión de clientes), ya que podrá verse amenazado por otros comportamientos que atacan contra su propio funcionamiento, por ejemplo, haciendo que la ejecución de tales programas sea mucho más lenta¹³⁸³, lo que deviene en un perjuicio o daño en sí mismo.

Constatado, pues, que estas acciones revisten idoneidad para poner en peligro seguridad del secreto de empresa, en su reserva, integridad o disponibilidad y que poseen asimismo carga lesiva, debe examinarse cuáles son las vías instauradas en el código penal vigente para sancionar tales acciones.

II) Las modalidades de acción analizadas (destrucción, alteración e inutilización) tampoco se hallan recogidas en los artículos 278 a 280 CP, destinados a regular la protección del secreto empresarial. La ausencia de previsión específica en los delitos arbitrados para su tutela constriñe a buscar un posible encaje en otros preceptos del código, que permita subsanar esta insoportable laguna.

¹³⁸² Para la definición de esta modalidades de comportamiento (borrar o cancelar, ocultar, inutilizar y alterar), vid. CORCOY, M., "Protección penal del sabotaje..." en MIR PUIG, S. (Comp.), **Delincuencia informática, op. cit.**, p. 166 y GONZÁLEZ RUS, J.J., "Protección penal de...", en **Jornadas sobre delincuencia...**, op. cit., pp. 532-533.

¹³⁸³ Esta modalidad de sabotaje puede llevarse a cabo mediante la introducción de un virus. Así, uno de los efectos de un «**virus program o virus**», que contenga subrutinas de consumo de tiempo, puede ser la disminución o reducción de velocidad de proceso de la máquina, (así, vid. entre muchos otros, CORCOY, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en MIR PUIG, S. (Comp.), **Delincuencia informática**, Barcelona, 1992, p. 152-153).

Al respecto, se suscitan dos vías de recogida de estos comportamientos, mediante la aplicación del artículo 200 CP y del artículo 264.2 CP.

a) La **primera hipótesis** propuesta radica en proyectar sobre estos comportamientos el ámbito de tutela del art. 200 CP, que contiene una cláusula de extensión de la tutela penal de la intimidad a los datos reservados de personas jurídicas¹³⁸⁴. En efecto, el art. 200 CP contempla una extraña cláusula en cuya virtud lo dispuesto en el capítulo I del título X (y, por tanto, en el art. 197.2 CP, que tipifica la alteración y modificación de los datos) es aplicable al descubrimiento, revelación o cesión de **datos reservados de personas jurídicas**.

Así, una interpretación amplia del citado precepto permitiría considerarlo idóneo para absolver una función subsidiaria, de recogida de conductas no abarcadas por el art. 278 CP, al precio de desconocer su ubicación sistemática entre los delitos contra la intimidad. Ellos supondría hacer extensivo el objeto del descubrimiento, revelación o cesión no sólo a los datos personales sino también a los datos que afectan a la actividad empresarial, que, lógicamente, obra en poder de personas jurídicas.

Sin embargo, no parece posible llevar a cabo la delimitación del art. 200 CP con desatención al bien jurídico protegido, lo que conduce a una interpretación restrictiva del precepto. Ello implicará que la alusión a los datos reservados de personas jurídicas sólo pueda proyectarse sobre **datos personales con trascendencia en la intimidad de las personas físicas** (por ejemplo, socios, directivos, empleados o terceras personas), que, sin embargo, son tratados y detentados por personas jurídicas, esto es, que

¹³⁸⁴ El art. 200 declara que «Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código».

obran en ficheros de personas jurídicas, que los gestionan y custodian¹³⁸⁵. En este sentido, una inteligencia articulada de la expresión típica con la que se cierra el art. 200 CP («...salvo lo dispuesto en otros preceptos de este código») conduce a un entendimiento de la misma como una **cláusula de advertencia** destinada a subrayar la existencia de otros preceptos en el código, enderezados a la salvaguarda de la información empresarial sensible y a la tutela de otros bienes jurídicos de naturaleza económica y, por tanto, dispar a la del bien jurídico intimidad que este capítulo I protege¹³⁸⁶. Así pues, debe desecharse la opción hermenéutica del art. 200 CP como fórmula subsidiaria idónea para cubrir el vacío normativo expuesto.

b) La **segunda hipótesis** radica en la aplicación del art. 264.2 CP, regulador del denominado delito de sabotaje informático, como tipo de cobertura de la citada laguna punitiva¹³⁸⁷. **De lege lata**, resulta posible que el art. 264.2 CP proyecte su ámbito típico sobre las conductas analizadas, puesto que castiga la conducta de quien destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos. Sin embargo, conviene ahondar en el estudio de diversos aspectos que su aplicación suscita, al objeto fundamental de corroborar la bondad de esta opción o, por el contrario, de formular una propuesta de reforma legislativa.

Desde luego, no se trata de un precepto exento de problemas y, aunque su estudio con profundidad asume un extraordinario interés, deberemos ceñirnos a plantear las dudas que su interpretación conlleva, a

¹³⁸⁵ En este sentido, vid., ampliamente, MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, op. cit., 2ª. ed., pp. 1003-1005.

¹³⁸⁶ Se trata de la expresión de la cláusula de subsidiariedad expresa, como regla de solución del concurso de normas.

¹³⁸⁷ El art. 264.2 CP establece que «La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».

los efectos que, en este momento, interesan por su vinculación al objeto de estudio principal.

Como cuestión previa, es necesario constatar dónde se sitúa el conflicto. Según el legislador, el delito de daños o sabotaje informático constituye un subtipo agravado del delito de daños en cosa ajena. Por tanto, parece que se trata de un «tipo equivalente» al delito de daños básico, construido atendiendo a la especial naturaleza del objeto¹³⁸⁸. Sin embargo, a partir de aquí, surgen varios problemas.

En primer lugar, cuando se repasa el código en busca del resto de posibles «tipos equivalentes» en los que se tenga presente esta misma singularidad del objeto, no se encuentran todos los que deberían estar, como ocurre, por ejemplo, en el ámbito de los delitos reguladores del secreto de empresa. Ante esta laguna normativa, automáticamente, el intérprete recalifica el precepto y es considerado, además de un subtipo agravado de la figura de daños, como una especie de tipo de recogida o “tipo-plantilla”, que permita cubrir los vacíos legales del resto del código, con lo que se desdibuja, en cierta forma, su propio contorno e idiosincrasia.

¹³⁸⁸ Frente a las distintas formas de delincuencia informática y, por tanto, ante el sabotaje informático, el legislador puede optar por diversas técnicas legislativas a la hora de afrontar la tipificación de nuevos preceptos penales con los que sancionar este tipo de criminalidad. Una de ellas consiste en la creación de lo que ROMEO CASABONA denomina «tipos de equivalencia», que complementen a los ya existentes, corrigiendo en la descripción de la acción típica las carencias detectadas en aquéllos, por ejemplo, en lo relativo a las modalidades comisivas y al objeto material del delito. Ésta es la vía seguida mayoritariamente en el ámbito del derecho comparado europeo, como se constata en los modelos alemán, italiano, portugués, austríaco y, también, en el español (así, vid. ROMEO CASABONA, C.M., “Los delitos de daños en el ámbito informático”, en *CPC*, nº 43, 1991, pp. 113-116 y, recientemente, ANDRÉS DOMINGUEZ, A.C., “Los daños informáticos en la Unión Europea”, en *LL*, nº 4725, 2 de febrero de 1999, pp. 2-3). Otra de las técnicas posibles se cifra, por el contrario, en la incriminación autónoma de todas aquellas conductas que puedan atentar contra el correcto funcionamiento de los sistemas informáticos. Ésta es la opción seguida, casi minoritariamente, en el ordenamiento francés.

Al asignar al delito esta función adicional, que afectará a la interpretación del mismo cuando se proyecte sobre esos otros comportamientos ayunos de protección, aparecen bastantes inconvenientes, que, aunque no puedan ser analizados en este momento, no sólo surgen en cuanto tipo de cobertura de las lagunas que generan los abusos informáticos contra otros bienes jurídicos, sino también cuando se aplica el precepto como subtipo del delito de daños.

La propia ubicación sistemática y la identificación del bien jurídico protegido desencadenan un sinfín de dudas, a las que se añaden las derivadas de la propia complejidad técnica de la materia sobre la que, en este caso, incide el código.

A) Empezando por las **cuestiones de orden más dogmático**, respecto del delitos de daños en cosa ajena, que se ubica en los delitos contra el patrimonio, la doctrina formula propuestas de distinto tenor, en las que se señala la propiedad ajena como objeto jurídico de protección¹³⁸⁹ o intereses de contenido económico no necesariamente identificables con el concepto de patrimonio **stricto sensu**¹³⁹⁰. Pues bien, al margen de la complejidad de identificar con precisión el bien jurídico protegido en el delito de sabotaje informático, lo cierto es que el art. 264.2 CP sanciona algunas **modalidades comisivas** (alteración, destrucción o inutilización de datos o programas) que pueden incidir sobre una pluralidad de bienes jurídicos de naturaleza heterogénea¹³⁹¹. En este sentido, podemos plantearnos cómo puede afectar

¹³⁸⁹ Así, JORGE BARREIRO, A., en RODRÍGUEZ MOURULLO, G., Dir., **Comentarios al...**, *op. cit.*, p. 748.

¹³⁹⁰ Así, vid. GUTIÉRREZ FRANCÉS, M.L., "Delincuencia económica...", en **Ámbito jurídico...**, *op. cit.*, p. 297. De modo análogo vid. CORCOY, M., "Protección penal del sabotaje..." en MIR PUIG, S. (Comp.), **Delincuencia informática**, *op. cit.*, p. 165, sostiene como bien jurídico protegido situaciones análogas a la propiedad.

¹³⁹¹ Por ejemplo, las siguientes conductas pueden incidir sobre diversos intereses: 1ª A, doctoranda en derecho penal, con el fin de perjudicar a B, compañero de escuela y también

el interés protegido por el delito de daños, sobre el que se construye el art. 264.2 CP, cuando deba decidirse, por ejemplo, si la introducción de un virus en la intranet de una empresa, que dificulta o entorpece el normal funcionamiento de la misma, constituye una conducta punible.

De otra parte, la configuración de los daños informáticos como subtipo agravado de los daños en cosa ajena implica, **a priori**, que comparten características comunes esenciales¹³⁹², incorporando la primera alguna

doctorando, introduce en el disco duro del ordenador de B un programa con un virus, que destruye todos los datos almacenados en el mismo, incluida su tesis doctoral, prácticamente terminada; 2ª Con el fin de desequilibrar una empresa de la competencia, A interfiere en su sistema informático, borrando todos los archivos relativos a la próxima estrategia de mercado; 3ª A, funcionario del Cuerpo Nacional de Policía, a cargo de los archivos informatizados secretos, borra una parte importante de datos, con el fin de que desaparezcan las diligencias relativas a un delito cometido por su novia; 4ª A penetra en los sistemas informáticos de un hospital y altera los datos de todas las consultas y pruebas médicas programadas para ese día, ocasionando serios perjuicios y un enorme caos; 5ª A, empleado de MUFACE, desde la terminal de su despacho, borra todos los datos relativos a las altas y bajas de dicho organismo; 6ª Con el fin de vengarse de la Facultad de Ingenieros de Telecomunicaciones, por no haber sido admitido en un postgrado, A penetra en su sistema informático, introduciendo un virus que contiene subrutinas de consumo de tiempo, de forma que los ordenadores que se utilizan como instrumento diario de trabajo, cada vez funcionan más lentamente; 7ª Para protestar contra el borrador de una nueva ley reguladora de internet, un grupo de hacktivistas envía masivamente peticiones al servidor del ministerio de justicia hasta bloquearlo, de forma que temporalmente deja de funcionar como es habitual. Pues bien, todos estos ejemplos comparten únicamente la modalidad comisiva. En la mayoría de ellos, la única vía de incriminación se cifra en la aplicación del delito de daños informáticos, aunque, incluso, algunos de los mismos resulten de difícil encaje en este precepto. En cualquier caso, el art. 264.2 CP no parece capaz de valorar adecuadamente la ofensividad o la gravedad de estas conductas en relación con los intereses en juego, que pueden ser muy distintos dependiendo de la concurrencia de diversas circunstancias. Antes bien, recuerda la regulación del antiguo capítulo VII del ACP (**Del descubrimiento y revelación de secretos**), que aglutinaba preceptos cuyo denominador común se cifraba en esa modalidad comisiva pero que albergaban la protección de bienes jurídicos de heterogénea naturaleza. Precisamente, ante esta dispersión legal se sostendrá la propuesta de reforma legislativa, destinada a introducir en el ámbito de los delitos relativos al secreto empresarial, alguna previsión que sancione específicamente los abusos informáticos, valorando la especificidad del objeto material del delito.

¹³⁹² En este sentido, MUÑOZ CONDE, F./GARCÍA ARÁN, M., **Derecho penal, Parte General**, 2ª ed., Valencia, 1996, p. 274, afirman que «tanto los tipos cualificados como los privilegiados son simples derivaciones del tipo básico, por lo que las reglas aplicables a éstos también son aplicables a aquéllos».

circunstancia que la cualifica y que motiva la elevación de la pena a imponer¹³⁹³. Ello hace que se generen diversos problemas.

El primer escollo radica en decidir si el artículo 264.2 CP debe cumplir la exigencia típica, prevista en el tipo básico (art. 263 CP) y sobre la que sí se construye el art. 264.1 CP, de que se haya producido un **daño cuantificable económicamente**, superior a cincuenta mil pesetas. Sin que reine unanimidad doctrinal al respecto¹³⁹⁴, en nuestra opinión, no parece que indispensablemente el art. 264.2 CP deba someterse al cumplimiento de este requisito, aunque puede suponer una fuente de conflictos y un serio obstáculo en la aplicación del precepto.

En el caso de que efectivamente se exija el requisito de un perjuicio superior a la cuantía de cincuenta mil pesetas, surge el segundo inconveniente, cifrado en valorar monetariamente el perjuicio que causa la destrucción, alteración o inutilización de los datos. Así, por ejemplo, cómo puede valorarse económicamente la conducta de quien provoca en el sistema informático de una empresa, en la que sus extraordinarios beneficios dependen de la rapidez con la que oferta sus productos al mercado (pongamos por caso Inditex), perjuicios consistentes en ver reducida la velocidad de proceso de algunas máquinas utilizadas por los trabajadores de la empresa o de todo el sistema¹³⁹⁵.

¹³⁹³ Vid., en igual sentido, ANDRÉS DOMINGUEZ, A.C., "Los daños informáticos en la Unión Europea", en **LL**, nº 4725, 2 de febrero de 1999, p. 3.

¹³⁹⁴ A favor de la exigencia de que el daño causado sea superior a cincuenta mil pesetas, vid. GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), **Curso de derecho penal español, Parte especial, P.I, op. cit.**, pp. 758-759 y JORGE BARREIRO, A., en RODRÍGUEZ MOURULLO, G., Dir., **Comentarios al...**, **op. cit.**, p. 752; en contra, vid. GUTIÉRREZ FRANCÉS, M.L., "Delincuencia económica...", en **Ámbito jurídico...**, **op. cit.**, p. 298.

¹³⁹⁵ Según los ejemplos sugeridos anteriormente, cómo puede evaluarse la introducción de un virus que borra una tesis doctoral a punto de terminarse, o cómo se evalúa la alteración, por mera diversión, de los turnos de guardias, descanso, vacaciones, etc. de los trabajadores de un centro hospitalario o la introducción de un virus en el sistema en el

También reviste complejidad, en algunos supuestos, el cumplimiento del **requisito típico** cifrado en que las acciones típicas recaigan sobre datos, programas o documentos electrónicos **ajenos**. En esa medida, las conductas de destrucción, alteración o inutilización de la información que sean ejecutadas por el titular del secreto no podrán formar parte del ámbito de tutela del precepto. Así, por ejemplo, en los casos en que se trate de secretos de empresa cuyo objeto se cifre en un programa de ordenador, si es el titular quien lleva a cabo el comportamiento de alteración o destrucción no se cumplirá el requisito típico de ajenidad y la conducta no será constitutiva de un delito de daños informáticos¹³⁹⁶. Ejemplo.

Por último, debe señalarse que las **penas** previstas para estas modalidades típicas son de prisión de uno a tres años y multa de doce a veinticuatro meses. Así, se otorga un tratamiento punitivo de menor gravedad para conductas que pueden resultar tan o, incluso, más lesivas para el bien jurídico que las previstas en el art. 278.1 CP, en su primer y su segundo inciso.

Las incoherencias y objeciones que desvela el sucinto análisis crítico acometido impiden arrojan cierta confusión acerca de la naturaleza jurídica del delito. Esto es, parece que, en realidad, el delito de sabotaje informático no se conforma como un subtipo agravado equivalente al delito de daños, sino que se trata de una figura autónoma con caracteres propios, con lo que su inserción en el título destinado a los delitos contra la propiedad aún resulta más perturbadora.

sistema informático de una agencia de seguridad privada, que, provoca, la anormalidad en su utilización y funcionamiento.

¹³⁹⁶ Acerca de la titularidad de los programas de ordenador, vid. art. 97 LPI.

B) A ello deben añadirse las **dificultades técnicas** inherentes a la materia, que dificultan una adecuada descripción de los comportamientos típicos. Al respecto, se van a plantear algunas cuestiones dudosas que el mismo suscita.

De una parte, el delito de daños informáticos prevé como objeto material los datos, programas o documentos electrónicos y no hace ninguna referencia al funcionamiento de los sistemas. El resultado es que no aparecen contemplados separadamente los efectos de muy diversa entidad que puede producir, por ejemplo, un virus. En este sentido, no reviste igual gravedad que el resultado del sabotaje sea la aparición de un mensaje en pantalla, o bien la reducción de la velocidad de proceso de la máquina o bien la destrucción total de los datos o información que contiene el ordenador. De ahí que quizá el código debería distinguir, como mínimo, entre los ataques que tienen como objeto la destrucción o inutilización de los datos o programas y los ataques que se proyectan sobre el funcionamiento del sistema y que se cifran en perturbaciones, molestias o alteraciones en el correcto funcionamiento del mismo.

Desde luego, aunque la actuación sobre el funcionamiento del sistema no está prevista específicamente, no parece conflictiva la subsunción de esta conducta puesto que los virus informáticos modifican los programas ejecutables a los que contaminan y, en esa medida, supondrán, al menos, una alteración de los datos que componen el programa. Aunque lo deseable quizá sería un tratamiento diferenciado.

Por otro lado, tampoco resulta sencilla la interpretación de la acción típica de «alteración», puesto que, prácticamente, cualquier actuación sobre el ordenador supone una modificación del sistema e incluso de los datos, como, por ejemplo, ocurre con los clusters. Quizá una redacción más precisa

podría evitar complicaciones a la hora de determinar cuándo estamos en presencia de una alteración o de una modificación relevante desde la perspectiva penal.

En conclusión, las consideraciones expuestas permiten constatar que el delito de sabotaje informático procura al bien jurídico protegido en los delitos relativos al secreto de empresa una tutela asistemática. Entre las diversas vías posibles para la protección jurídica de la información contenida en redes, soportes o sistemas informáticos, una de ellas consistiría en corregir las deficiencias que perviven en algunos ámbitos del código, introduciendo específicas previsiones en esos preceptos, a fin de que puedan valorarse los perfiles propios de los intereses protegidos (incluido el propio delito de daños informáticos). Y otra vía más arriesgada se cifraría en trasladar el precepto a un capítulo de nueva creación, que recogiese éste y todos los demás atentados contra los sistemas informáticos, entre los que podría hallarse incluso la incriminación del mero intrusismo informático.

Pues bien, el legislador español ha optado por la creación de un precepto regulador de los daños informáticos. Desde luego, no puede ahondarse en el análisis acerca de la oportunidad o bondad de este tipo concreto en la lucha contra la criminalidad informática, pero sí debe cuestionarse su idoneidad para reprimir los ataques al bien jurídico protegido --por los delitos reguladores del secreto de empresa-- derivados de modalidades comisivas cifradas en abusos informáticos¹³⁹⁷.

En conclusión, pues, a tenor de la laguna existente en los art. 278 a 280 CP para reprimir las fuentes de peligro que estos abusos técnicos suscitan sobre el bien jurídico y del encaje forzado e insatisfactorio que tales

¹³⁹⁷ En contra, vid. CORCOY, M., “Protección penal del sabotaje...” en MIR PUIG, S. (Comp.), *Delincuencia informática, op. cit.*, p. 176.

conductas tienen en el art. 264.2 CP, se estima conveniente formular alguna propuesta de reforma legislativa.

III) Así, concretando esta propuesta, a nuestro parecer, sería aconsejable la creación de un tipo o modalidad específica, dirigida a sancionar las conductas de alteración, destrucción o inutilización de la información que conforma el objeto del secreto de empresa. Esto es, un tipo inserto en los preceptos reguladores de la violación de secretos y destinado a proteger el bien jurídico —en este caso, el interés del empresario en mantener la reserva de ciertas informaciones, que habitualmente se almacenan en equipos informáticos y se transmiten por circuitos telemáticos—frente a estos nuevos focos de riesgo que emergen tras la implantación generalizada de las nuevas tecnologías en el ámbito empresarial. De hecho, el legislador ha previsto estos riesgos en otros ámbitos, como, por ejemplo, en los delitos contra la intimidad, en los que específicamente se dedica un precepto a regular los abusos informáticos (art. 197.2 CP). Análogamente, se han tenido presentes estas **formas de ataque** en los delitos relativos a la infidelidad de documentos y violación de secretos en el ámbito de los delitos contra la Administración Pública (art. 413 y 414 CP), aunque estos preceptos presenten algunas limitaciones para aprehender esas acciones de destrucción, alteración u ocultación, cuando sean fruto de ataques informáticos.

En esta medida, la formulación de dicho precepto deberá tener en cuenta la especial configuración del objeto material del delito y del propio bien jurídico y arbitrar en atención a estas peculiaridades una tutela adecuada. Ello supone que para proteger eficazmente la información empresarial sensible contenida en redes o soportes informáticos deberá tenerse en cuenta la dificultad de evaluar el perjuicio. De ahí que no resulte adecuado incorporar como elemento típico la producción de una lesión o

daño cuantificable económicamente, ya que ni necesariamente el perjuicio que puede producirse es patrimonial y, generalmente, reviste carácter difuso, diferido o indirecto¹³⁹⁸. Al respecto, tampoco parece que la posible inclusión de un elemento subjetivo del injusto deba cifrarse únicamente en el ánimo de perjudicar¹³⁹⁹. Sin poder abundar en el examen particularizado sobre el elemento subjetivo del injusto, puede aventurarse que, de postularse la incorporación de un componente subjetivo al tipo de abusos informáticos, se cifraría en la finalidad de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto, de tenor similar al sugerido en la modalidad de acción relativa al apoderamiento¹⁴⁰⁰. Aunque, la previsión de dicho elemento en este ámbito, merece, sin duda, una más detenida reflexión.

De igual modo, quizá convenga meditar acerca de la relevancia que debería asumir en la configuración del precepto la circunstancia de que, en gran parte de los casos, estas conductas sean ejecutadas por empleados de

¹³⁹⁸ El impacto de un ataque informático puede incidir sobre distintos ámbitos de la empresa. Así, puede afectar a lo que podrían considerarse propiamente activos (hardware, software), incidir sobre su propia organización (repercusiones en el mercado, en su imagen, en el personal) o sobre su planificación (proyectos de inversión futuros, planes de fusión). Así, en un hipotético cálculo del impacto **cuantitativo** de un ataque, debería valorarse el coste directo sobre activos de recuperación del ataque, de reposición, de instalación de mecanismos de seguridad y el coste indirecto cifrado en la pérdida de productividad, en la dedicación de personal de mantenimiento y operación a reinstalación o puesta a punto. En cuanto al posible cálculo del impacto **cualitativo**, deberían evaluarse las pérdidas orgánicas (fondo de comercio, personal), las pérdidas funcionales (productividad, presencia en el mercado, credibilidad, confianza) (así, vid. esCERT-UPC-CANet: <http://escert.upc.es>).

¹³⁹⁹ En cambio, se muestran partidarios de que estas conductas siempre se llevan a cabo con ánimo de producir un perjuicio patrimonial, según ROMEO CASABONA, C.M., “Delitos informáticos...”, en *Informática..., op. cit.*, p. 438 o un perjuicio empresarial evaluable económicamente, según GUTIÉRREZ FRANCÉS, M.L., “Delincuencia económica...”, en *Ámbito jurídico..., op. cit.*, p. 293. A nuestro parecer, no necesariamente ha de ser así. Sin duda, en la mayor parte de los casos, que suelen ser acometidos por empleados en situaciones de conflictos laborales o tras haber sido despedidos, el sujeto activo busca la venganza y, en esa medida, perjudicar al empresario; pero, no puede olvidarse que, en otros casos, aunque minoritarios, puede pretenderse el beneficio propio o de tercero, mejorando la propia situación competitiva, por ejemplo.

¹⁴⁰⁰ Vid. supra epígrafe relativo al elemento subjetivo.

la propia empresa (denominados *insiders* o *intraneus*)¹⁴⁰¹. En efecto, los propios trabajadores gozan de una situación especialmente privilegiada para saber dónde se halla la información, acceder a ella y reproducirla, alterarla, destruirla o inutilizarla. Esto es, tienen a su alcance la posibilidad de acceder a la información reservada con mayor facilidad.

IV. «Difusión», «revelación» y «cesión».

1. Consideraciones preliminares.

Las acciones típicas de difusión, revelación y cesión, cuyo contenido interesa examinar, se corresponden con diversas modalidades de conducta, que se vertebran sobre estos verbos nucleares pero que configuran tipos de injusto distintos.

De una parte, la difusión, revelación o cesión constituye la conducta nuclear del tipo agravado (art. 278.2 CP¹⁴⁰²), construido sobre las acciones anteriormente analizadas (apoderamiento, control audiovisual clandestino y control ilícito de señales de comunicación), que configuran el tipo básico (art. 278.1 CP). Por tanto, se trata de la difusión, revelación o cesión de un secreto previamente descubierto, al que **se ha accedido ilícitamente**.

¹⁴⁰¹ Como se acaba de señalar, actualmente, y sin pasar por alto las dificultades inherentes al conocimiento de este ámbito de la criminalidad, que constituye una de las parcelas donde la «cifra negra» es superior, es comúnmente aceptado que la mayor parte de comportamientos ilícitos relativos a la informática se llevan a cabo por personas vinculadas, de algún modo, a las empresas, esto es, empleados de confianza, programadores, técnicos, operadores. De hecho, según un reciente estudio norteamericano, el 80% de las infracciones relacionadas con la informática, tienen como autores a empleados de la propia empresa, que, por lo general, buscan la venganza o el provecho ilícito.

¹⁴⁰² El artículo 278.2 CP establece que: «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».

De otro lado, estas acciones se corresponden, de igual modo, con los comportamientos previstos en el art. 279.1 CP¹⁴⁰³, que consagra un tipo autónomo. En este caso, la diferencia respecto de la anterior modalidad de conducta estriba en que **el acceso** a la información --que, posteriormente, se difunde, revela o cede-- **ha sido lícito**. En esta modalidad, el núcleo del injusto radica en que la difusión, revelación o cesión se lleva a cabo con infracción de un deber (legal o contractual) de guardar reserva.

Por último, estas modalidades de acción típica son, asimismo, las previstas en el art. 280 CP --reverso, de hecho, de estas acciones que, como se analizará, revisten la naturaleza de ser de participación necesaria--¹⁴⁰⁴. Así, el sujeto que, tras recibir la información por parte de quien realiza la revelación, difusión o cesión de los arts. 278.2 y 279.2 CP, no se limita a dicha recepción, sino que, a su vez, difunde, revela o cede el secreto recibido, lleva a cabo una «revelación en cadena», es decir, estas acciones que ahora se analizan.

2. Concepto de «difundir», «revelar» y «ceder».

Las acciones de difusión, revelación y cesión, previstas en las modalidades objeto de estudio, se insertan en una estructura que se corresponde con la de un **tipo mixto alternativo**. En esta medida, la inclusión de estos tres términos, coordinados disyuntivamente (difusión, revelación o cesión de secretos de empresa), parece sugerir que se trata de modalidades

¹⁴⁰³ El artículo 279.1 CP declara que: «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».

¹⁴⁰⁴ El artículo 280 CP manifiesta que: «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».

de comportamiento de contornos o perfiles distintos entre sí. En primer lugar, en el intento de precisar su contenido y, a la vez, de desgajar su singular ámbito de proyección, se abordará el significado de las acciones de mayor arraigo en nuestro código (difusión y revelación) y, posteriormente, se analizará la modalidad de reciente incorporación (cesión), estrechamente vinculada a la generalización de las nuevas tecnologías y, en concreto, de la informática.

I) Con arreglo a una interpretación gramatical, «difundir» significa hacer que una noticia o doctrina sea conocida o aceptada por más gente, es decir, divulgar, esparcir, expandir o propagar¹⁴⁰⁵, y por «revelar» se entiende decir o hacer saber cosas que se mantenían secretas, dar a conocer cosas ocultas, esto es, descubrir, comunicar¹⁴⁰⁶. Según lo anterior, el matiz distintivo más notable radicaría tal vez en el mayor ámbito de conocimiento o, en otras palabras, en la mayor publicidad, que parece implicar la difusión, aunque, ciertamente no constituya un criterio determinante.

Pues bien, como quiera que una interpretación gramatical de estos conceptos no aporta herramientas suficientes para deslindarlos con nitidez, quizá convenga examinar si se trata de elementos normativos, cuya interpretación reclama una indagación en fuentes jurídicas. Así, centrando el examen en el propio ámbito penal, se observa que son términos habitualmente utilizados por el legislador en la regulación de la violación de secretos.

¹⁴⁰⁵ MOLINER, M., *Diccionario de uso del español*, 2ª ed. Madrid, 1998; segunda acepción y sinónimos de ésta.

¹⁴⁰⁶ MOLINER, M., *Diccionario de uso del español*, 2ª ed. Madrid, 1998; primera y segunda acepción.

Empezando el estudio por los delitos contra la intimidad, los frecuentes paralelismos que presenta la estructuración típica de éstos con los delitos objeto de estudio merecen, de nuevo, una atención detallada¹⁴⁰⁷. Así, el art. 197.3 CP tipifica la difusión, revelación o cesión de los secretos personales descubiertos, esquema en el que parece haberse inspirado la incriminación de estas conductas en el ámbito de los secretos de empresa, pero que, a los efectos que ahora interesan, no aporta ningún matiz que permita distinguir entre sí las conductas de difusión y de revelación. Sin embargo, el art. 199 CP, que sanciona la infracción de deberes de sigilo profesionales y laborales, contiene una regulación dispar que merece reflexión¹⁴⁰⁸. De una parte, en el inciso primero, en que se sanciona el

¹⁴⁰⁷ En efecto, obsérvese que la estructura típica es muy similar. De una parte, se incrimina el **acceso ilícito** a la información (en el caso de los delitos contra la intimidad, con apoderamiento de documentos y de efectos personales en el art. 197.1 y con acceso directo a los datos en el art. 197.2; en los delitos relativos al secreto de empresa, en el art. 278.1 CP). A continuación se concibe un tipo agravado, proyectable a los anteriores tipos básicos, de difusión, revelación o cesión a terceros de los secretos descubiertos (arts. 197.3, primer apartado y art. 278.2 CP). Además, se contempla, asimismo, la difusión, revelación o cesión de secretos a los que se ha accedido lícitamente, con obligación de sigilo profesional o laboral (arts. 199, 200 y 279.1 CP). Por último, se incrimina la revelación, difusión o cesión de la información por quien conoce su origen ilícito y no ha tomado parte en su descubrimiento, es decir, el reverso de las conductas analizadas (art. 197.3, segundo inciso y art. 280 CP). Así pues, el paralelismo es evidente. De hecho, parece que el legislador, en algunas ocasiones, simplemente ha trasladado la estructuración típica de los delitos contra la intimidad al ámbito de la protección de los secretos de empresa, sin atender a la especificidad del bien jurídico protegido y del propio objeto material, que no resultan análogos a los de la intimidad. Así, por ejemplo, parece haber ocurrido en la traslación de las acciones típicas que ahora se analizan o en la remisión que lleva a cabo en el art. 278.1 CP a las modalidades del 197.1, sin tener en cuenta que las acciones previstas no resultan plenamente equiparables, como tampoco lo es el marco extrapenal que alimenta aquellos delitos (fundamentalmente, la antigua LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos personales (LORTAD), recientemente derogada por la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que constituye la norma básica reguladora de las garantías y la protección de la intimidad personal, respecto del tratamiento de datos, tenga o no carácter automatizado). Por otra parte, el legislador, en cambio, no parece haber acudido al marco extrapenal que le proporciona la LCD en este ámbito.

¹⁴⁰⁸ El artículo 199 CP establece que «1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses. 2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años».

quebrantamiento de deberes de discreción en la esfera laboral, se incrimina la **revelación** de secretos ajenos; en cambio, en la regulación del secreto profesional, en el segundo párrafo, se opta por tipificar la **divulgación** de los secretos.

Ante la diversidad de consecuencias interpretativas que cabría extraer de esta distinta descripción típica, la doctrina (MORALES PRATS¹⁴⁰⁹, JORGE BARREIRO¹⁴¹⁰) ha reclamado la necesidad de que las acciones de «revelar» y «divulgar» sean interpretadas como sinónimos, dada la incoherencia que supondría exigir un plus o incremento de injusto en la conducta típica de revelación del secreto profesional (art. 199.2 CP), que, al prever la **divulgación** de los secretos, no quedaría perfeccionada si la intimidad del tercero no es conocida por un amplio número de personas. Por tanto, en esta sede, la única conclusión inferible es la equiparación valorativa entre ambas.

En el ámbito de los delitos contra la Administración Pública, el art. 417.1 CP, relativo a la revelación de secretos por autoridad o funcionario público, emplea indistintamente, en su primer párrafo, los términos referentes a la revelación y a la divulgación¹⁴¹¹. De modo que la consecuencia deducida anteriormente se ve ratificada.

¹⁴⁰⁹ Así, vid. MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, *op. cit.*, 2ª. ed., p. 993. Anteriormente, esta incorrección técnica ya fue advertida y censurada por MORALES PRATS respecto del art. 189 del PANCP, que incurría en el mismo error, al emplear el término divulgar respecto del secreto profesional y el verbo revelar en la regulación del deber de sigilo profesional (así, vid. “Privacy y reforma penal: la Propuesta de Anteproyecto de Nuevo Código Penal de 1983”, en **Documentación jurídica**, núm. 37/40, Monográfico dedicado a la Propuesta de Anteproyecto del Nuevo Código Penal, vol. 1, Madrid, 1983, p 615).

¹⁴¹⁰ JORGE BARREIRO, A., “Descubrimiento y revelación...”, en *op. cit.*, pp. 264-266 y, posteriormente, en “El delito de revelación de secretos (profesionales y laborales)”, en **LL**, nº 4038, 17 de mayo de 1996, p. 5.

¹⁴¹¹ El artículo 417 CP establece que: «1. La autoridad o funcionario público que revelare secretos o informaciones de los que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados, incurrirá en la pena de multa de doce a dieciocho meses e

Y, por último, inserto en los delitos relativos a la defensa nacional, el art. 599 CP, contempla como subtipo agravado en su párrafo segundo, que la revelación consista en «dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión»¹⁴¹².

En suma, a tenor de lo expuesto, no parece inferible una nítida distinción legal entre las conductas de revelación y divulgación; por otra parte, la diferenciación formulada –entre revelación y difusión-- en el ámbito de los delitos relativos a la defensa nacional, no parece abstraíble para ser predicada al resto de delitos, dado el diferente bien jurídico y régimen configurador que esos delitos asumen y que resulta de cariz diverso a los propuestos en los delitos reguladores de la vulneración del secreto de empresa. En esta medida, el examen detallado de los verbos empleados en el vigente código al tipificar estas modalidades comisivas ***no permite inferir un criterio sistemático unívoco y uniforme.***

Ello nos lleva ya a indagar el contenido de estas acciones directamente en el contexto del resto de elementos típicos que configuran los arts. 278.2 y 279.1 CP y, en especial, a tenor de la relevancia que puede asumir en la conculcación del bien jurídico propuesto.

Por lo que se refiere al contenido de las acciones de difusión y de revelación, se postula de modo mayoritario por la doctrina un diverso

inhabilitación especial para empleo o cargo público por tiempo de uno a tres años. Si de la revelación a que se refiere el párrafo anterior resultara grave daño para la causa pública o para tercero, la pena será de prisión de uno a tres años, e inhabilitación especial para empleo o cargo público por tiempo de tres a cinco años».

¹⁴¹² El artículo 599 CP establece que: «La pena establecida en el artículo anterior se aplicará en su mitad superior cuando concorra alguna de las circunstancias siguientes: (...) 2º. Que la revelación consistiera en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión».

contenido entre ambas, de modo que la «revelación» se produciría cuando el secreto se comunica a un número determinado de personas y la «difusión» equivaldría a una divulgación o propagación del secreto entre una pluralidad de personas¹⁴¹³.

Sin duda, pues, la difusión se ve asociada a la idea de una mayor publicidad¹⁴¹⁴. Y, en esa medida, dado que la divulgación generalizada supondrá la notoriedad del secreto, acarreará, asimismo, la pérdida del valor o ventaja que su mantenimiento en reserva otorgaba al titular y, de hecho, al desaparecer por completo la reserva se producirá la destrucción del bien económico que representa el secreto. De ahí que se suela equiparar su divulgación pública con un mayor peligro o una mayor carga de desvalor¹⁴¹⁵.

Así pues, **de lege data**, la incorporación de ambas modalidades (revelación y difusión) permite reprimir tanto la comunicación del secreto a sujetos concretos y determinados como la divulgación generalizada del mismo.

¹⁴¹³ Así, distinguen este doble ámbito en el sentido expuesto, GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), **Curso de derecho penal, op. cit.**, p. 800; SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., **Comentarios al..., op. cit.**, p. 804; MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), **Curso de derecho penal económico**, Madrid, 1998, p. 284; CARRASCO ANDRINO, M.M., en **La protección penal..., op. cit.**, pp. 206 y 217 y FERNÁNDEZ SÁNCHEZ, M.T., **Protección penal..., op. cit.**, pp. 232-271. Por el contrario, se muestran partidarios de una interpretación, como mínimo, de los términos revelar y divulgar como sinónimos o equivalentes, TERRADILLOS BASOCO, J., **Derecho penal..., op. cit.**, pp. 171-172; BAJO FERNÁNDEZ, M./BACIGALUPO, S., **op. cit.**, p. 507 y SERRANO GÓMEZ, A., **Derecho penal, Parte Especial**, Madrid, 1997, p. 432. A nuestro parecer, y sumándonos a la posición de estos últimos autores, también las tres acciones deben ser interpretadas como términos equivalentes, tal como se sostendrá en la interpretación crítica que se lleva a cabo.

¹⁴¹⁴ En este sentido, respecto del art. 197.3 CP, vid. MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código..., op. cit.**, 2ª. ed., p. 983.

¹⁴¹⁵ Así, vid. MORENO CÁNOVAS, A./RUIZ MARCO, F., **Delitos socioeconómicos, op. cit.**, p. 131; CARRASCO ANDRINO, M.M., en **La protección penal..., op. cit.**, p. 206 y ROBLEDO VILLAR, A., **Delitos contra el patrimonio y el orden socioeconómico**, Barcelona, 1997, p. 379.

Por último, debe analizarse ya el contenido de la última de las acciones previstas en estos delitos y, posteriormente, tras concluir su análisis, será el momento de formular una interpretación crítica acerca del ámbito –diverso o, por el contrario, equiparable-- que todas estas acciones asumen.

II) Por lo que se refiere al concepto de la tercera acción típica, «ceder» significa dar o dejar voluntariamente a otro el disfrute de cierta cosa, privándose de ella¹⁴¹⁶.

A diferencia de las conductas anteriores, se trata de una conducta de reciente incorporación en el ámbito penal, que ni aparecía en el anterior código ni en los proyectos anteriores al vigente. Sin embargo, el término «ceder» asume un significado normativo en otros sectores del derecho, como en el ámbito civil y mercantil, cuyo validez no resulta, sin embargo, proyectable a los delitos objeto de estudio¹⁴¹⁷.

Se ha sugerido que la cesión, a diferencia de las otras acciones, implica siempre la entrega del soporte material que contiene el secreto¹⁴¹⁸. Sin embargo, intentar discernir las acciones típicas separando la **puesta en conocimiento** del secreto de la **puesta a disposición del soporte** en el que se

¹⁴¹⁶ MOLINER, M., *Diccionario de uso del español*, 2ª ed. Madrid, 1998; primera acepción.

¹⁴¹⁷ En el ámbito del derecho civil, aparece referido a la cesión de bienes, a la cesión de contratos o a la cesión de créditos. Sin embargo, en todos estos casos, el cedente sólo puede ser el titular de los bienes, de los derechos o de la posición jurídica, lo que invalida su proyección a los delitos objeto de estudio. En el campo mercantil, se suele emplear la expresión cesión de know-how, para aludir a un contrato en cuya virtud se transmiten los datos que conforman el objeto del know-how. Así que tampoco parece posible interpretar el término «cesión» con arreglo a este significado normativo. Vid., en este sentido, ampliamente, CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 215.

¹⁴¹⁸ SERRANO GÓMEZ, A., *Derecho penal, op. cit.*, p. 432.

exterioriza el secreto, significa desconocer la naturaleza intrínseca de intangibilidad e inmaterialidad que caracteriza al secreto de empresa¹⁴¹⁹.

Así pues, de nuevo, se acudirá al propio código en la búsqueda de criterios que contribuyan a perfilar su significado jurídico.

El término cesión aparece, asimismo, contemplado en los delitos relativos a la intimidad (art. 197.3, primer inciso CP), ámbito en el que, según ha advertido ya la doctrina¹⁴²⁰, parece previsto para ser proyectado técnicamente al tipo básico de abusos informáticos (art. 197.2 CP). Sin duda, éste es el campo en el que resulta, en mayor medida, concebible aludir a la «cesión de datos». Es, precisamente, la normativa sectorial extrapenal relativa a la protección de datos personales, la que proporciona una definición de dicho término que sí cobra validez en los delitos objeto de estudio.

La vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), regula en sus artículos 11 y 27 la cesión de datos personales¹⁴²¹. Previamente, el art. 3.i) de la LOPD define la cesión o comunicación de datos como «toda revelación de datos realizada a una persona distinta del interesado» y, posteriormente, el art. 11.1 LOPD, que contiene el principio fundamental aplicable a las cesiones de datos personales, aparece rubricado como «Comunicación de

¹⁴¹⁹ En este sentido, vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 217.

¹⁴²⁰ MORALES PRATS, F., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código...*, *op. cit.*, 2ª. ed., p. 983.

¹⁴²¹ Acerca de la regulación de la cesión de datos personales en la nueva LOPD, vid. MIRALLES MIRAVET, S./BACHES OPI, S., “La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos”, en *LL*, nº 5306, 11 mayo 2001, pp. 2 y ss. y TÉLLEZ AGUILERA, A., *Nuevas tecnologías. Intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Madrid, 2001, pp. 151 y ss.

datos». Así pues, en la LOPD se utilizan indistintamente los términos «cesión» y «comunicación». Análogamente, en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, únicamente se menciona la «comunicación de datos» [arts. 2 b) y 7 f)], para hacer referencia a la transmisión o intercambio de datos por medios electrónicos, sin aludir ni incorporar, en ningún momento, el término «cesión»¹⁴²².

En esta medida, parece que el término cesión al que aluden los arts. 278.2 y 279.1 CP es equiparable o equivalente a la transmisión, comunicación o revelación de los datos que componen el secreto de empresa, independientemente de que conlleve la entrega del soporte en que se contiene el secreto.

Pues bien, desde luego, si el resto de elementos típicos y, en concreto, la incidencia específica que estas conductas revisten sobre el bien jurídico devienen indispensables a la hora de aprehender el significado jurídico de su contenido, una interpretación atenta a los mismos resulta, aún, de mayor importancia en la formulación de cualquier consideración crítica. De ahí que, a nuestro parecer, precisamente la singularidad de estas acciones (difusión, revelación y cesión) en los delitos objeto de estudio, permita sugerir algunas consideraciones que justificarán el significado jurídico que, **de lege lata**, se les otorga, de una parte y que contribuyan a reflexionar sobre la formulación de posibles propuestas **de lege ferenda**, de otra.

¹⁴²² Asimismo, MIRALLES MIRAVET, S./BACHES OPI, S., “La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos”, en **LL**, nº 5306, 11 mayo 2001, n. 9, consideran que el término «comunicación» resulta más apropiado que el término «cesión», para aludir a situaciones de transmisión de datos por medios electrónicos.

En primer lugar, parece que la incorporación de dichas acciones en los arts. 278.2 y 279.1 CP obedece a la adopción automática de la estructura típica prevista en el ámbito de los delitos contra la intimidad, que, como se sabe, no sólo se enderezan a la protección de un bien jurídico distinto, sino que tienen un objeto material de naturaleza diversa a la que posee el secreto de empresa. En buena lógica, pues, en algunos casos, no parece aconsejable proponer, sin mayor reflexión, un entendimiento en los mismos términos de estas conductas en ambos sectores.

Como se sabe, el secreto de empresa es un bien esencialmente económico, de naturaleza inmaterial o intangible, sustentado sobre la situación de reserva. De ahí que, incontrovertiblemente, su divulgación pública suponga la notoriedad del secreto y su destrucción como bien económico. Ahora bien, debe tenerse en cuenta que, una vez comunicado el secreto, aunque sólo sea a una única y concreta persona, se pierde el control que se poseía sobre el mismo y se corre el riesgo ya de que esa persona pueda reproducirlo a otros o ya de que pueda decidir utilizarlo en provecho propio o ajeno o a fin de perjudicar a un tercero. De ahí que la revelación a una o varias personas determinadas genere, asimismo, el elevado riesgo de la pérdida del valor que el secreto asume para su titular.

En esta medida, dada la peculiar naturaleza de este tipo de información, no parece que el concepto o la idea de publicidad sea absolutamente equiparable en el ámbito de los delitos contra la intimidad y en los delitos relativos a la protección del secreto de empresa, puesto que, en este caso, en cuanto se da a conocer la información desaparece el control sobre la misma y el interés económico del empresario se ve puesto en peligro.

En segundo término, la experiencia pone de manifiesto que, en el ámbito objeto de estudio, lo que se produce con mayor frecuencia no es una difusión generalizada de la información secreta (por ejemplo, a través de medios de comunicación, como sí suele ocurrir en el ámbito de los delitos relativos a la intimidad, lo que explicaría quizá que se desgaje conceptualmente la divulgación), sino la revelación a personas concretas y determinadas¹⁴²³. Es decir, **se revela intencionadamente a un destinatario seleccionado de antemano**, ya porque se trata de un competidor directo especialmente interesado, ya porque el que revela está a punto de convertirse él mismo en competencia junto con alguien a quien comunica la información, o bien porque se ejecutan las conductas que, en función del destinatario, puedan resultar más perjudiciales o dañosas para el empresario, como suele ocurrir en el caso de empleados descontentos que actúan por venganza. Es decir, en estos casos, las conductas que resultan más peligrosas para el bien jurídico y que incorporan un plus de desvalor suelen ser, precisamente, lo que, según la terminología empleada por el código, se consideraría un supuesto de **revelación**, caracterizado, en teoría, por revestir menor peligrosidad¹⁴²⁴.

Así pues, a nuestro parecer, atendiendo a la peculiaridad del objeto material y del bien jurídico protegido, el núcleo del injusto material radica en **la comunicación del secreto empresarial a cualquier persona no autorizada para entrar en conocimiento del mismo, en cuya virtud el secreto se introduce en la esfera de disponibilidad de ese sujeto no autorizado**¹⁴²⁵. A

¹⁴²³ Sin embargo, de otra opinión parecen MORENO CÁNOVAS, A./RUIZ MARCO, F., **Delitos socioeconómicos, op. cit.**, p. 131, quienes afirman que «la esencia de las tres formas comisivas (difusión, revelación y cesión) suponen un incremento del número de personas que acceden al conocimiento del contenido de la información confidencial».

¹⁴²⁴ En contra, vid. CARRASCO ANDRINO, M.M., en **La protección penal...**, op. cit., p. 206.

¹⁴²⁵ Vid., en este sentido, VIGNA, P.L./DUBOLINO, P., voz: «Segreti (reati in materia di)», en **Enciclopedia del Diritto**, vol. XLI, Giuffrè, 1989, p. 1042.

partir de aquí, la conducta de comunicación puede ejecutarse **por cualquier medio** --ya sea oralmente o por escrito, por vía analógica o digital y, por tanto, con entrega del soporte material en el que se exteriorice el secreto o sin él- y dirigirse al público en general o a terceros determinados, entre los que también pueden hallarse personas pertenecientes a la organización del titular del secreto que, sin embargo, por razón del cargo no debían tener acceso a dicha información¹⁴²⁶.

La inteligencia de que lo relevante, desde el punto de vista de la lesividad, no es tanto la destrucción de la reserva sino la pérdida del valor del secreto para su titular conduce a radicar el injusto en **cualquier acto de comunicación del secreto a un sujeto no autorizado para su conocimiento**, en el bien entendido que quien lleva a cabo dicha conducta se aprovecha indebidamente del esfuerzo ajeno, actúa sin basarse en las propias prestaciones y falsea las reglas de juego del mercado, que sólo puede tolerar aquellas conductas (incluidas las de revelación o difusión del secreto) que respondan a una mayor eficiencia.

De ahí que la comunicación del secreto a un tercero que no pueda ofender el bien jurídico protegido en estos delitos (por ejemplo, por tratarse de la revelación a una persona del ámbito familiar), devenga una conducta atípica por mor del principio de ofensividad o de lesividad¹⁴²⁷. La caracterización del bien jurídico desde el derecho de la competencia desleal ha permitido encuadrar el objeto de protección en el ámbito de la competencia económica y, en particular, en la esfera de libertad de ejercicio de una actividad económica. De ahí que se haya circunscrito al interés

¹⁴²⁶ Vid, en igual sentido, MASSAGUER FUENTES, J.J., **Comentario a la ley...**, *op. cit.*, p. 393.

¹⁴²⁷ El **bien jurídico** ofrece un criterio material decisivo en la construcción de la teoría jurídica del delito y, por tanto, en la interpretación de los tipos penales en particular (así, vid. COBO DEL ROSAL, M./VIVES ANTÓN, T.S., **Derecho penal**, *op. cit.*, p. 315).

económico del empresario en mantener la reserva de ciertos conocimientos, persiguiéndose además con su tutela fomentar el esfuerzo innovador. No se protege, pues, la libertad de voluntad de mantener en secreto cualquier conocimiento, ni la intimidad del empresario ni un derecho subjetivo de éste a una determinada posición jurídica. En buena lógica, pues, la realización de un hecho sin capacidad de dañar el bien jurídico formulado determinará la ausencia de antijuridicidad material y, por tanto, la atipicidad de la conducta. En esta medida, la revelación o comunicación del secreto, en el sentido normativo que reclaman los arts. 278.2 y 279.1 CP, no se conformará con la efectuada a cualquiera, sino que deberá limitarse a las comunicaciones con trascendencia en el marco competitivo en el que se inserta la prohibición penal y, por tanto, el sujeto pasivo o receptor de la revelación deberá encontrarse entre las personas relevantes en ese contexto¹⁴²⁸. Ahora bien, a partir de aquí, parece difícil formular reglas apriorísticas con validez general. De ahí que no parezca exigible que el destinatario de la información deba ser necesariamente un empresario competidor (como reclamaba el modelo profesional del derecho de la competencia, pero no el vigente modelo social consagrado por la LCD, ex arts. 1, 2 y 3) o pertenecer al mismo círculo laboral del sujeto que revela. Por otra parte, también parece difícil la fijación de criterios apriorísticos determinantes de la ausencia de riesgo de que el tercero receptor de la comunicación lo transmita o lo emplee, como podría ser que se trate de alguien ajeno a la esfera laboral o profesional del sujeto activo. De ahí que el enjuiciamiento de la conducta deba efectuarse en el supuesto concreto a tenor de si la conducta posee capacidad para ofender el bien jurídico protegido.

Retomando el análisis crítico del significado de las acciones, parece que, de hecho, el legislador también ha querido equiparar valorativamente

¹⁴²⁸ Análogamente, vid. a CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, pp. 208-209.

estas acciones de difusión, revelación y cesión, puesto que no ha previsto un diverso trato punitivo, a diferencia de lo que ocurre en la revelación de secretos e informaciones relativas a la defensa nacional¹⁴²⁹. Ahora bien, si ello es así, entonces tal vez convendría emplear un único verbo capaz de aprehender la dimensión antijurídica de estos comportamientos, en la línea seguida por los arts. 284 y 285 del PCP 1992 y los arts. 273 y 274 PCP 1994, que sólo contemplaban la acción de «revelar»¹⁴³⁰. Así, se evitaría el recurso a forzadas interpretaciones, a la postre disfuncionales, que doten de sentido propio a cada una de las modalidades típicas incorporadas en los preceptos, como aconseja el principio de vigencia.

Al efecto, diversas opciones parecen igualmente idóneas. De una parte, se muestra adecuado el término acuñado por la normativa sectorial de carácter civil, de la que tendría que haber partido el legislador penal, que considera desleal **la divulgación, sin autorización de su titular, de secretos** a los que se ha tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente (art. 13.1 LCD). Éste es el término adoptado, asimismo, por el art. 39. 2 del Acuerdo ADPIC, que, en relación a la información no divulgada, **sanciona la divulgación a terceros sin consentimiento de su titular**. De otro lado, también parece sugerente la incorporación de una única acción como la de **comunicación** (así, por ejemplo, el § 17 UWG alemana) o, incluso, la de

¹⁴²⁹ Por el contrario, esta agravación de la conducta de difusión de secretos e informaciones relativas a la defensa nacional permite a CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, p. 206, llegar a la conclusión contraria. De ahí que, a juicio de esta autora, los términos difusión y revelación previstos en el art. 279.1 CP asuman un significado diverso.

¹⁴³⁰ En sentido contrario, la previsión exclusiva del término «revelar» fue objeto de crítica, reclamándose al respecto, una mayor precisión terminológica y, en concreto, la incorporación de la acción de «difusión»; así ha sido específicamente reivindicado por MASSAGUER FUENTES, J.J., “Los secretos industriales y comerciales y su transmisión: régimen jurídico”, en FONT GALÁN, J.I./NAVARRO CHINCHILLA, J.J./VÁZQUEZ GARCÍA, R.J., *op. cit.*, p. 183, respecto del PCP 1992 y en “Los delitos contra el orden socio-económico (I): los delitos relativos a la propiedad industrial, al mercado y a los consumidores”, en **Foro canario**, 1994, p. 196, en cuanto al PCP 1994.

revelación (así, el art. 623 CP italiano y art. 6-bis l.i. italiana), cuya previsión en exclusiva ahorra esfuerzos interpretativos y permite captar la esencia del comportamiento injusto.

En conclusión, a nuestro parecer, **de lege lata**, los términos de difusión, revelación y cesión acuñados por el legislador en estas modalidades de conducta asumen un significado similar, en cuyo interpretación no se han podido encontrar criterios unívocos que deslinden con claridad sus respectivos ámbitos de aplicación y que, por ello, deben ser interpretados como términos sinónimos o equivalentes. Probablemente, el legislador ha preferido incluir todas las acciones analizadas, aunque redunde en una incorrección lingüística, para evitar lagunas legales. Así, se persigue tipificar tanto la revelación generalizada como la revelación **intuito personae**. Sin embargo, debe partirse de lo que es realmente importante, a saber, que hay un emisor y un receptor --o varios-- y que se castiga la conducta del emisor. Por lo que atañe a la cesión, de nuevo parece que el legislador para evitar lagunas y, dado que quizá la **revelación** se asocia a la comunicación **meramente intelectual** de la información pero no a través del soporte, decide incorporar también el término ceder, para que, indubitadamente, tengan cabida los supuestos de revelación mediante la entrega del soporte que contiene el secreto. A tenor pues de la conclusión expuesta, parece aconsejable que, **de lege ferenda**, se emplee un único término capaz de aprehender el núcleo del injusto, que se cifra en la conducta de comunicación del secreto a un tercero no autorizado.

Una vez concluida la interpretación crítica de las acciones de difusión, revelación y cesión, conviene ya profundizar en algunas de las características que, intrínsecamente, suscitan. Las dos secuencias o modalidades de conducta en las que se insertan los verbos analizados comparten la estructuración que, en virtud de diferentes criterios (atendiendo

al sujeto activo, a la modalidad de comportamiento, a la relación o afección del bien jurídico, entre otros múltiples), a continuación, se propone. No se desconoce que las características singulares de cualquier clasificación típica y, en concreto, de las que siguen, han de ser extraídas desde dentro del tipo y desde su peculiar composición.

Así pues, es desde los concretos tipos de injusto (arts. 278.2 y 279.1 CP), a través de un análisis de las conductas a ellos incorporadas y de la ofensa que éstas comportan, desde donde se constatará, en primer lugar, la naturaleza de delitos pluripersonales o de participación necesaria que ambos ostentan¹⁴³¹. Sin embargo, como quiera que la caracterización que se formula resulta compartida por ambos tipos de injusto, se ha optado por incluir su estudio como cuestiones comunes.

3. Caracterización típica: delitos pluripersonales o de participación necesaria.

Atendiendo al sujeto activo, las modalidades de conducta, previstas en los arts. 278.2 y 279.1 CP, se caracterizan por requerir la presencia de varias acciones de diferentes personas. La estructura típica de estos delitos se corresponde, pues, con la de los delitos pluripersonales o de participación necesaria¹⁴³², en la medida en que los tipos se hallan de tal forma

¹⁴³¹ Así es reclamado específicamente por COBO DEL ROSAL, M./VIVES ANTÓN, T.S., *Derecho penal, op. cit.*, p. 440. Vid., ampliamente, sobre estas estructuras típicas y las consecuencias que de ellas se derivan, RODRÍGUEZ PUERTA, M.J., *El delito de cohecho: problemática jurídico-penal del soborno de funcionarios*, Pamplona, 1999, pp. 91 y ss.

¹⁴³² También denominados delitos de participación impropia. En la literatura española, se contempla mayoritariamente esta categoría, aunque con un contenido o entendimiento de la misma diferente, según se expondrá; así, vid., en nuestra doctrina, COBO DEL ROSAL, M./VIVES ANTÓN, T.S., *Derecho penal, op. cit.*, p. 439; MIR PUIG, S., *Derecho penal, Parte general, op. cit.*, p. 208; LUZÓN PEÑA, D.M., *Curso de derecho penal, Parte general, op. cit.*, p. 304; OCTAVIO DE TOLEDO Y UBIETO, E./HUERTA TOCILDO, S., *Derecho penal, Parte general, op. cit.*, p. 49; MUÑOZ CONDE, F./GARCÍA ARÁN, M., *Derecho penal, Parte General*, 2ª ed., Valencia, 1996, p. 276 y, en la literatura alemana, vid. JESCHECK, H.H., 630

concebidos que para su realización resulta necesaria conceptualmente la intervención de más de una persona¹⁴³³, sin que ninguna de ellas sea víctima del delito. Conviene, en este momento, desgranar la definición propuesta en algunas de las notas caracterizadoras, que, doctrinalmente, les son asignadas¹⁴³⁴, al objeto de constatar más detalladamente si dichas notas concurren en estos delitos.

En primer lugar, para la realización del tipo se necesita la **inevitable contribución de dos o más personas**. Así, la especial configuración de estos delitos y, en concreto, el verbo típico empleado en ellos precisa para ser ejecutado la intervención de más de un sujeto, esto es, el que revela, difunde o cede la información secreta y el que la recibe, sin que ninguno de ellos sea víctima del delito¹⁴³⁵. Y, en concreto, éstos serían delitos de participación

Tratado de Derecho Penal, Parte General, traducción y adiciones de Derecho español por MIR PUIG, S y MUÑOZ CONDE, F., vol. II, Barcelona, 1981, pp. 968-971.

¹⁴³³ Así, vid. JESCHECK, H.H., **Tratado de Derecho Penal, Parte General**, traducción y adiciones de Derecho español por MIR PUIG, S y MUÑOZ CONDE, F., vol. II, Barcelona, 1981, p. 968.

¹⁴³⁴ Así, vid., en nuestra doctrina, COBO DEL ROSAL, M./VIVES ANTÓN, T.S., **Derecho penal, op. cit.**, pp. 440-441 y, exhaustivamente, RODRÍGUEZ PUERTA, M.J., **El delito de cohecho: problemática jurídico-penal del soborno de funcionarios**, Pamplona, 1999, pp. 102 y ss.

¹⁴³⁵ Ésta, sin embargo, parece ser la caracterización que asume la doctrina, mayoritariamente, en nuestro país. Con arreglo a este entendimiento, en los casos de participación necesaria, aunque el tipo requiere la intervención activa de varios sujetos, algunos no son autores o auténticos sujetos activos del delito, sino sólo sujetos activos materiales de la acción, pero su colaboración es precisamente forzada por el atutor o está viciado su consentimiento; de ahí que sean por ello impunes, pues en muchos casos ese aparente sujeto activo es realmente sujeto pasivo del delito; así, vid. LUZÓN PEÑA, D.M., **Curso de derecho penal, Parte general, op. cit.**, p. 304 y, análogamente, vid. MIR PUIG, S., **Derecho penal, Parte general, op. cit.**, p. 208; MUÑOZ CONDE, F./GARCÍA ARÁN, M., **Derecho penal, Parte General, op. cit.**, p. 276 y OCTAVIO DE TOLEDO Y UBIETO, E./HUERTA TOCILDO, S., **Derecho penal, Parte general, op. cit.**, p. 49.

necesaria de los denominados de encuentro o con conductas contrapuestas¹⁴³⁶.

Además, estas diversas conductas de los distintos sujetos **forman parte del total acontecer lesivo descrito por la ley**. Efectivamente, a pesar de que el tipo sólo haga mención explícita de las acciones de revelar, difundir o ceder el secreto empresarial, contempla implícitamente la de recibir dicho secreto. En este sentido, el que grita en una habitación vacía la proporción exacta en la que se mezclan los ingredientes en la fórmula de la coca-cola no lleva a cabo una conducta de revelación o difusión penalmente relevante, puesto que no han concurrido los elementos que implícita o conceptualmente reclama el tipo.

De ahí que sea necesario para la consumación del tipo que la información revelada, difundida o cedida, esto es, comunicada, haya llegado a conocimiento de un tercero no autorizado, siendo irrelevante que efectivamente éste haya alcanzado su total comprensión o intelección. No se exige que el destinatario utilice el secreto o lo comprenda (así, la información puede estar cifrada o resultar de extraordinaria complejidad), sino sólo que el tercero haya tomado conocimiento efectivamente del secreto y, por tanto, esté, a su vez, **en disposición** o **en condiciones** de divulgarlo o de utilizarlo¹⁴³⁷.

Por último, tanto el tipo de injusto previsto en el art. 278.2 como el descrito en el art. 279.1 CP contienen una única figura de delito y protegen

¹⁴³⁶ Acerca de las divergente configuración entre los delitos pluripersonales de convergencia y los delitos pluripersonales de encuentro, vid. RODRÍGUEZ PUERTA, M.J., **El delito de cohecho...**, *op. cit.*, pp. 103-104.

¹⁴³⁷ Acerca de la innecesariedad de la comprensión del secreto por parte del receptor de la información, para entender consumada la conducta, vid. infra el análisis del **iter criminis** de cada modalidad típica.

un mismo bien jurídico protegido, que **sólo una vez resulta lesionado**, lo que, desde el punto de vista lesivo, conlleva la perpetración de un único delito. En efecto, se trata de una figura, en cuya especial estructura típica varias personas llevan a cabo conductas distintas (uno revela y el otro recibe la información), pero tendentes a la obtención de una misma finalidad, a saber, lograr la transmisión de un secreto empresarial.

Esta especial configuración típica demanda que se lleve a cabo una diferenciación entre el plano típico y lesivo y el reproche personal que es necesario afirmar en el delito. El reproche penal es personalísimo, autónomo e independiente y afecta tan sólo a cada uno de los sujetos en particular, por lo que, como advierten COBO/VIVES¹⁴³⁸, los sujetos participantes en estos delitos no tienen por qué correr idéntica suerte en cuanto a la culpabilidad y a la concreción de la punibilidad.

Con arreglo a esa distinción entre ambos planos, se constata que, en los delitos analizados, el legislador establece la punibilidad de la conducta de determinados intervinientes, mientras que la de otros permanece impune. Así, mientras que la conducta de quien revela un secreto, al que se ha accedido ilícitamente o, por el contrario, legítimamente pero con deber de reserva, merece sanción penal, en cambio, la conducta de quien recibe la información no es objeto de idéntica valoración y, si se limita a recibir tal información, no es merecedora de reproche penal. Únicamente, la conducta del sujeto receptor de la información resultará reprochable si, además de tomar conocimiento efectivo de la información, a su vez, la divulga o la utiliza en provecho en propio, en cuyo caso vendrá en aplicación el art. 280 CP, en el bien entendido de que el sujeto haya actuado con conocimiento del origen ilícito de la información. Así, de algún modo, el art. 280 CP, con los matices

¹⁴³⁸ COBO DEL ROSAL, M./VIVES ANTÓN, T.S., *Derecho penal, op. cit.*, p. 441. Vid., en igual sentido, RODRÍGUEZ PUERTA, M.J., *El delito de cohecho...*, *op. cit.*, pp. 105-106.

expuestos, podría considerarse el reverso de las acciones de difusión, revelación o cesión¹⁴³⁹.

En esta medida, si se hubiese previsto una consecuencia jurídica para el receptor de la información, éste respondería como autor, en cuanto sujeto activo del delito, aunque su aportación sea la de sujeto pasivo de la acción, en cuyo caso sería un delito –de participación necesaria– de naturaleza pluripersonal¹⁴⁴⁰. De ahí que la decisión del legislador de no establecer un reproche penal para el mismo, omitiendo cualquier referencia a esta posibilidad, determine que, de llevarse a cabo la conducta típica, la recepción de la información devenga una conducta impune. No parece que de ello quepa inferir que se trata de una protección penal establecida en su beneficio o consecuencia lógica de su condición de objeto de protección de la norma, sino que, político-criminalmente, se estima preferible limitar la intervención penal a aquellos supuestos, en los que el destinatario de la

¹⁴³⁹ Una estructura análoga es la prevista en los arts. 417.1 y 418 CP. El art. 417.1 CP incrimina la revelación de secretos o informaciones públicas u oficiales por autoridad o funcionario público. Y el art. 418 CP sanciona la conducta del particular que aprovecha para sí o para un tercero el secreto o la información privilegiada que obtuviere de un funcionario público o autoridad. Pues bien, como sostienen MORALES PRATS, F./RODRÍGUEZ PUERTA, M.J., en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código...**, *op. cit.*, 2ª. ed., pp. 1902 y 1905, el art. 417.1 CP se configura como un delito de participación necesaria, en el que deviene indispensable la intervención de más de un sujeto, el que revela y el que recibe la información. Ahora bien, en este delito sólo resulta incriminada la conducta del funcionario que revela, mientras que la conducta del receptor de la información, si se limita a tal recepción, permanece impune. Sólo en la medida en que el particular receptor de la información, además de recibirla, se aproveche de ella, su conducta resultará punible con arreglo al art. 418 CP, que constituye el reverso del art. 417.1 CP. De igual modo, en el ámbito de los delitos contra la intimidad, el art. 197.3, primer inciso CP, tipifica la difusión, revelación o cesión de los datos o hechos descubiertos y, en su segundo párrafo, incrimina la conducta del receptor de dicha información, siempre que, habiendo actuado con conocimiento de su origen ilícito, a su vez, revele, difunda o ceda la información recibida. Así pues, el art. 197.3, segundo inciso CP, también constituye el reverso del art. 197.3, primer apartado, CP, que requiere implícitamente para su consumación la intervención de varias personas y también se configura, en esa medida, como un delito de participación necesaria.

¹⁴⁴⁰ Acerca de la individualización de la categoría del ilícito pluripersonal, vid. RODRÍGUEZ PUERTA, M.J., **El delito de cohecho...**, *op. cit.*, pp. 93-98. Esta naturaleza de delito pluripersonal de encuentro revisten algunas modalidades de cohecho, vid., sobre el particular, la autora citada, pp. 143 y ss.

comunicación ilícita del secreto empresarial lleve a cabo actos idóneos para poner en peligro el bien jurídico, como pueden ser la propia divulgación del secreto o su utilización en provecho propio¹⁴⁴¹.

Desde luego, la bondad político-criminal de esta opción debe ser objeto de una reflexión más detenida, atenta a una pluralidad de criterios en los que, en este momento, no se puede ahondar. Sin embargo, no parece una decisión desacertada, atendiendo al bien jurídico protegido en estos delitos. El interés económico del empresario en mantener la reserva de ciertos conocimientos, como concreta estrategia competitiva, no se ve igualmente afectado por la conducta de quien recibe el secreto ilícitamente y se limita a su mero conocimiento, sin llevar a cabo ninguna conducta más -- con la potencial peligrosidad que ello conlleva y que se tiene en cuenta y de ahí la conveniencia de una más profunda reflexión--, que por la conducta de quien habiéndolo recibido, decide divulgarlo de nuevo «en cadena» o hacer uso de él en provecho propio.

Así pues, en cuanto al tratamiento jurídico-penal del receptor de la información, puede concluirse que si la intervención de dicho sujeto no sobrepasa la que requiere el tipo, su conducta permanece impune¹⁴⁴². Y la desborda o sobrepasa cuando no se limita a recibir sino que lleva a cabo las conductas previstas en el art. 280 CP.

Esta caracterización de las conductas de revelación, difusión o cesión como delitos de participación necesaria, en los que sólo es punible, por

¹⁴⁴¹ Quizá en el trasfondo político-criminal de dicha opción se persiga facilitar el descubrimiento y la denuncia por parte de quien se limita a recibir la información.

¹⁴⁴² Así, vid., en derecho comparado, JESCHECK, H.H., *Tratado de Derecho Penal, Parte General, op. cit.*, p. 969 y, en nuestra doctrina, MIR PUIG, S., *Derecho penal, Parte general, op. cit.*, p. 208.

decisión legal, la conducta del sujeto que revela el secreto, conlleva un régimen jurídico especial en dos aspectos. Uno de ellos es el relativo a la tentativa, al que más tarde se hará referencia autónoma. Y el otro concierne al régimen de la participación. Por lo que se refiere a este segundo aspecto, de admitirse la calificación de estos delitos como de participación necesaria, la conducta del sujeto destinatario de la información no podrá sancionarse a través de las reglas generales de la participación¹⁴⁴³. Precisamente, estas estructuras típicas persiguen excepcionar dicho régimen general, en la medida en que se excluye, si así lo ha establecido el código penal, la sanción de uno de los sujetos que intervienen en el delito. Y, por ello, nunca podrá considerarse partícipe en el delito del otro al sujeto receptor de la información, cuya conducta devendrá pues impune salvo en los supuestos del art. 280 CP, a los que ya se ha hecho mención¹⁴⁴⁴.

Sin embargo, será posible apreciar y sancionar cualquier conducta de participación de un tercero (inducción, cooperación necesaria o complicidad) siempre que pueda probarse que se dirigen a auxiliar al sujeto cuya conducta es punible (esto es, el emisor de la información). En efecto, nada impide la participación de un tercero en la conducta del sujeto activo del delito, en cuyo caso será de aplicación el régimen general de la participación. Así, por ejemplo, la conducta de intermediación en la revelación, difusión o cesión de un secreto poniendo en contacto al sujeto con un tercero interesado en adquirirlo, puede ser castigada como una conducta de cooperación, en la medida en que el sujeto que intermedia

¹⁴⁴³ En sentido contrario, vid. GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal, op. cit.*, p. 801, en cuya opinión, los supuestos de coautoría y participación de extraños se resolverán conforme a los criterios generales, de forma que el coautor responderá por el art. 280 y también los cómplices, porque el concurso de normas que se plantea entre su participación en este delito y el 280, como autor, debe resolverse a favor del segundo.

¹⁴⁴⁴ Así, vid. RODRÍGUEZ PUERTA, M.J., *El delito de cohecho...*, *op. cit.*, p. 104.

participa en la revelación cometida por el sujeto activo del delito, emisor de la información.

Una de las cuestiones más problemáticas, sin embargo, reside en aquellos supuestos en los que la conducta del sujeto que recibe el secreto viene precedida de un comportamiento de inducción. En esos casos, el destinatario de la comunicación es, a la vez, autor –impune-- de un delito de revelación de secretos y partícipe –en concepto de inductor-- en el mismo delito, pero cometido por el emisor de la información.

En tales casos, sancionar la conducta menos grave de inducción resulta, en cierta forma, contradictorio con la impunidad que se predica de la conducta más grave de autoría en el delito, que, sin embargo, permanece impune¹⁴⁴⁵. Aun así, lo cierto es que dicha cuestión despierta serios interrogantes y reclama una reflexión más detenida¹⁴⁴⁶.

¹⁴⁴⁵ De otra opinión parece MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 87, al resolver el supuesto planteado por QUERALT JIMÉNEZ, J.J., en *Derecho penal español, Parte especial, Delitos contra los intereses individuales y colectivos*, 3ª ed., Barcelona, 1996, pp. 214-215, relativo al sujeto que obligado a guardar reserva de un secreto de la empresa para la que trabaja es contratado por los responsables de la empresa competidora con el fin de que aquél transmita a éstos la información reservada. A juicio de MARTÍNEZ-BUJÁN, el sujeto obligado responderá por un delito de revelación (art. 279.1 CP), puesto que, con independencia de que quepa estimar que utiliza el secreto en provecho propio (art. 279.2 CP), lo cierto es que también divulga el secreto a los responsables de la empresa competidora, y éste último es prevalente en el concurso de leyes suscitado entre ambos. Por su parte, los responsables de la empresa competidora serán inductores del delito especial propio del art. 279.1 CP ejecutado por el obligado al secreto. A nuestro parecer, de calificar la conducta del sujeto como una revelación del art. 279.1 CP, el comportamiento de los competidores debería quedar impune. Por su parte, QUERALT JIMÉNEZ considera que los representantes de la empresa competidora son autores de una conducta de acceso ilícito, prevista en el art. 278.1 CP, puesto que «se sirven de un instrumento doloso no cualificado para el delito del art. 278 y, al mismo tiempo, son cooperadores necesarios del delito de vulneración de la confidencialidad del art. 279.2 CP. Se produce, por tanto, un concurso de leyes, que deberá ser resuelto por el principio de especialidad», a favor del art. 278.1 CP. «En cuanto al sujeto privilegiado, el quebrantador de la confidencialidad, si bien es instrumento doloso no cualificado en el delito de los responsables de la empresa, sigue cometiendo el delito del art. 279.2 CP, que, por ser más especial, será el que resultará aplicable». Según advierte ya MARTÍNEZ-BUJÁN, los responsables de la empresa competidora podrían ser autores de un acceso ilícito (art. 278.1 CP) si verdaderamente concurriese en el sujeto obligado la condición de instrumento al servicio de aquéllos, lo que no parece que sea el caso en la hipótesis sugerida. Sin perjuicio

4. Estructura típica: delitos de mera actividad o delitos de resultado.

La decisión acerca de si la estructura típica adoptada por estos delitos se corresponde con la de mera actividad o con la de resultado debe adoptarse desde la atención al injusto material de estos delitos.

Según se ha expuesto ya¹⁴⁴⁷, en este trabajo, el resultado se concibe como un efecto, material o ideal, consecuencia de la conducta y distinto de la misma, generalmente posterior pero a veces simultáneo a ella¹⁴⁴⁸. Por tanto, aunque el resultado no se limita a un entendimiento del mismo en sentido naturalístico, tampoco se conforma con su identificación como mero suceso distinto de la acción y separable de ésta al menos mentalmente.

Adoptando, pues, la concepción expuesta, debe averiguarse si, en los tipos de injusto que se sustentan sobre la revelación, difusión y cesión de los secretos, efectivamente, se requiere algún efecto de la acción en cuanto suceso y efecto separable de ésta, en cuyo caso podrá afirmarse su configuración como un delito de resultado o si, por el contrario, se trata de una acción o una actividad que se agota en sí misma, sin necesidad de

de que, al abordar la última de las modalidades típicas (utilización), estos supuestos serán analizados con mayor detalle, valga anticipar que, en nuestra opinión, en el ejemplo propuesto, el sujeto obligado lleva a cabo una conducta de revelación o de utilización del secreto, dependiendo de lo que después se indicará y los competidores, probablemente, responderán, también como autores del delito de utilización del secreto –recibido fruto de una comunicación ilícita—previsto en el art. 280 CP.

¹⁴⁴⁶ En nuestra doctrina, vid., sobre el particular, CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, pp. 323 y ss.

¹⁴⁴⁷ Vid. supra, comentario a las acciones de apoderamiento y de control audiovisual clandestino y de control ilícito de señales de comunicación.

¹⁴⁴⁸ LUZÓN PEÑA, D.M., **Curso de derecho penal, Parte general, I**, Madrid, 1996, p. 307.

ningún elemento ulterior para su conclusión efectiva, con lo que se configurará como un delito de mera actividad¹⁴⁴⁹.

La identificación del núcleo material del injusto típico se ha cifrado en cualquier acto de comunicación del secreto a un sujeto no autorizado para su conocimiento, en cuya virtud la información secreta ***entra en la esfera de disponibilidad de ese tercero no autorizado***. En este caso, pues, a diferencia de las conductas anteriormente analizadas (apoderamiento e interceptación), la revelación engendra un proceso autónomo de disposición y conocimiento del secreto por parte del tercero que recibe la información. Y, precisamente, cuando ese proceso de disponibilidad de la información se produce, a consecuencia de una conducta de revelación, es el momento en que puede entenderse conculcado el bien jurídico protegido y, por ende, plenamente consumado el delito.

En efecto, la toma de conocimiento por un tercero y, por tanto, la incorporación a su esfera de disponibilidad de la información hace peligrar el interés económico del empresario en mantener la reserva de esos conocimientos, como forma más idónea de organizar su empresa y mantener su posición competitiva en el mercado. De ahí que cuando esa comunicación del secreto empresarial, por condiciones subjetivas (referidas al receptor de la información) u objetivas (afecta a conocimientos parciales e inservibles), no puede provocar la pérdida de valor que el secreto asume

¹⁴⁴⁹ En cualquier caso, como sugerentemente advierte ROXIN, C., *Derecho penal, Parte general, T. I, Fundamentos. La estructura de la teoría del delito*, 2ª ed. trad. por LUZÓN PEÑA/DÍAZ Y GARCÍA CONLLEDO/DE VICENTE REMESAL, Madrid, 1999, p. 327, no todos los tipos se pueden encuadrar claramente en los delitos de resultado o de actividad, sino que, incluso, a veces hay que distinguir caso por caso. Así, por ejemplo, las lesiones son un delito de mera actividad si consisten en una bofetada, pero son un delito de resultado si se producen lanzando una piedra.

para su titular y, en concreto, que la información sea ulteriormente divulgada o utilizada, la conducta no será típica¹⁴⁵⁰.

Así pues, en la medida en que se requiere la producción de un ulterior suceso, cifrado en ese proceso de conocimiento y disponibilidad por parte del tercero receptor de la información, parece que los tipos de injusto analizados (arts. 278.2 y 279.1 CP) que contemplan la revelación o la difusión de secretos empresariales se configuran como delitos de resultado¹⁴⁵¹.

5. Momento de la consumación.

La conducta típica consiste en la revelación, difusión o cesión del secreto empresarial a terceros no autorizados. La consumación de estas modalidades de acción típica se produce cuando se pone en conocimiento de otra persona la información, sin que sea necesario que el receptor alcance la total intelección o comprensión de la misma¹⁴⁵². Es decir, para

¹⁴⁵⁰ Vid., en este sentido, MASSAGUER FUENTES, J.J., *Comentario a la ley...*, *op. cit.*, p. 394.

¹⁴⁵¹ Así, estas condutas son entendidas como resultado material del delito por MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, pp. 75 y 80, por lo que se refiere a los arts. 278.2 y 279.1 CP, respectivamente; GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal, op. cit.*, p. 800; SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., *Comentarios al...*, *op. cit.*, p. 807, respecto al art. 279.1 CP; CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 207; MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos, op. cit.*, p. 139, en lo que se refiere al art. 279.1 CP; ROBLEDO VILLAR, A., *Delitos contra el patrimonio y el orden socioeconómico*, Barcelona, 1997, pp. 379 y 382, en cuanto a los arts. 278.2 y 279.1 CP, respectivamente; FERNÁNDEZ SÁNCHEZ, M.T., *Protección penal...*, *op. cit.*, pp. 272 y ss.; por el contrario, MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), *Curso de...*, *op. cit.*, p. 287, afirma, en el análisis del tipo básico previsto por el art. 279.1 CP, que «El art. 279 no se configura como un delito de resultado material o de lesión, pues la descripción del tipo no contiene el resultado que se considera prohibido».

¹⁴⁵² Unánimemente la doctrina considera irrelevante la comprensión del secreto para entender consumado el delito; así, vid. BAJO FERNÁNDEZ, M./SUÁREZ GONZÁLEZ, C., en BAJO FERNÁNDEZ, M./PÉREZ MANZANO, M./SUÁREZ GONZÁLEZ, C., *Manual de derecho penal, Parte especial...*, *op. cit.* p. 382; TERRADILLOS BASOCO, J., *Derecho penal...*, *op. cit.*, p. 172; MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte*

que la comunicación se entienda consumada basta con que se ponga al destinatario en condiciones o en disposición de una ulterior divulgación o utilización del secreto revelado, sin que sea exigible que efectivamente lo comprenda, lo utilice o le reporte una ventaja¹⁴⁵³.

De nuevo, la identificación del bien jurídico tutelado en el legítimo interés económico del empresario permite captar la configuración típica de estas conductas. Es decir, la protección del secreto empresarial no se basa en la tutela de la intimidad del empresario o en la de su patrimonio industrial, sino en la preservación de los resultados del propio esfuerzo. De ahí que no se proteja la situación de secreto per se, como manifestación de la libertad de voluntad, sino como situación fáctica de la que deriva el valor económico que esa información ostenta para su titular. No se protege la posesión de secretos empresariales frente al resto de empresarios, como posición jurídica absoluta, lo que determina la impunidad de aquellas revelaciones, difusiones o cesiones de secretos que no hayan sido realizadas abusivamente y, por tanto, no sean concurrencialmente reprobables. Sólo las revelaciones acometidas con apropiación de esfuerzo ajeno y sin actividad propia son capaces de ofender el bien jurídico protegido y de poner en peligro el valor que el secreto otorga a su titular.

De ahí que, desde la perspectiva del ataque que se produce sobre el bien jurídico protegido, se trate de **delitos de peligro**, que no reclaman para

especial, op. cit., pp. 76 y 82; BAJO FERNÁNDEZ, M./BACIGALUPO, S., **op. cit.**, pp. 509-510; GUTIÉRREZ FRANCÉS, M.L., "Notas sobre la delincuencia informática...", en ARROYO ZAPATERO, L./TIEDEMANN, K., **Estudios de derecho...**, **op. cit.**, p. 198; SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., **Comentarios al...**, **op. cit.**, p. 807; PRATS CANUT, J.M., "Descubrimiento y revelación de secretos...", en **Delitos relativos a la propiedad...**, **op. cit.**, p. 195; CARRASCO ANDRINO, M.M., en **La protección penal...**, **op. cit.**, p. 207 y MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), **Curso de...**, **op. cit.**, pp. 285 y 287.

¹⁴⁵³ Vid., en este sentido, MASSAGUER FUENTES, J.J., **Comentario a la ley...**, **op. cit.**, p. 393.

su consumación la efectiva lesión del interés económico del empresario. A nuestro parecer, la comunicación ilícita de la información empresarial reservada posee capacidad potencial para poner en peligro el bien jurídico. Cada vez que se revela un secreto, **se pierde el control** sobre la información comunicada y ésta entra a formar parte de la esfera de disponibilidad del destinatario de la información, de modo que se corre el riesgo de que éste, a su vez, pueda revelar en cadena el secreto o proceder a una ulterior utilización del mismo. Así que las acciones típicas de difusión, revelación o cesión poseen aptitud para poner en peligro la propia situación de reserva, lo que genera una peligrosidad o afectación suficientemente relevante para el propio bien jurídico. Se trata, por tanto, de **delitos de peligro hipotético**, puesto que los comportamientos analizados poseen una aptitud para producir la conculcación del bien jurídico, esto es, una idoneidad lesiva¹⁴⁵⁴.

Ahora bien, esa capacidad potencial **ex ante** para producir un peligro sobre el bien jurídico, deberá ser verificada en el caso concreto por el juez, sin que eso implique la constatación de un peligro concreto o de que la acción haya producido un resultado de peligro de lesión inmediata y próxima sobre el bien jurídico¹⁴⁵⁵.

¹⁴⁵⁴ Vid., en igual sentido, TERRADILLOS BASOCO, J., **Derecho penal...**, *op. cit.*, p. 168, respecto del art. 499 ACP y MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte especial**, *op. cit.*, pp. 75 y 81, respecto del art. 278.2 y 279.1 CP; por el contrario, éstos son entendidos como delitos de peligro abstracto por LANDECHO VELASCO, C.M./MOLINA BLÁZQUEZ, C., **Derecho penal español...**, *op. cit.*, p. 253, respecto del art. 279.1 CP; MOLINA BLÁZQUEZ, C., "La criminalización de la competencia desleal...", **PJ**, *op. cit.*, p. 246, respecto del art. 285 PCP 1992; JORDANA DE POZAS GONZÁLBEL, L., en CONDE-PUMPIDO FERRERIO, C. (Dir.), **Código penal, doctrina y jurisprudencia**, T. II; Madrid, 1997, p. 2981, en relación al art. 279. 1 CP; una postura análoga defiende CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, p. 212 y ss., que considera el delito previsto en el art. 279.1 CP como un delito de peligro abstracto o de peligrosidad **in re ipsa**, entendida como una peligrosidad inherente al tipo.

¹⁴⁵⁵ Defienden el carácter de delitos de peligro concreto PRATS CANUT, J.M., "Descubrimiento y revelación de secretos...", en **Delitos relativos a la propiedad...**, *op. cit.*, p. 195, por lo que se refiere al art. 278.2 CP; MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), **Curso de...**, *op. cit.*, pp. 285 y 287 y FERNÁNDEZ SÁNCHEZ, M.T., **Protección penal...**, *op. cit.*, pp. 272-273 y 299, respecto al art. 278.2 y 279.1 CP.

6. *Iter criminis*.

Según se ha expuesto, el momento de la consumación de estas modalidades de acción típica se produce cuando se pone en conocimiento de otra persona la información, sin que sea necesario que el receptor alcance la total intelección o comprensión de la misma. Esta caracterización de la modalidad de acción comentada, junto a la atribución a la misma de la condición de delito de resultado y de participación necesaria condicionan el análisis de las cuestiones relativas al *iter criminis*.

En primer lugar, al tratarse de un delito de resultado serán admisibles tanto la tentativa inacabada como la acabada. Un ejemplo de la primera lo encontramos en aquellos supuestos en los que el autor del delito se dispone a poner en circulación la información procediendo, por ejemplo, a reunirla en un archivo que posteriormente enviará o a introducirla en un sobre al que dará el mismo destino. Un ejemplo de la segunda se halla, por contra, en aquellos supuestos, en los que habiéndose dado curso a la información, ésta no llega a formar parte de la esfera de disponibilidad del destinatario. Así podría ocurrir si, pongamos por caso, no le llega el e-mail, porque yerra en la dirección o porque éste es interceptado por la policía judicial.

Estas formas imperfectas de ejecución deberán apreciarse desde el momento en que el sujeto emisor de la información da curso a la misma. Pese a tratarse de un delito de participación necesaria, no será indispensable, en el supuesto de ejecución imperfecta, la intervención de los dos sujetos implicados en el hecho delictivo. A diferencia de los delitos de participación necesaria, denominados de convergencia, en los de encuentro

—categoría a la que pertenece el delito de revelación de secretos—es posible y punible la tentativa unilateral¹⁴⁵⁶.

7. Penalidad.

8. La difusión, revelación o cesión omisivas.

La posibilidad de que estas modalidades de acción típica sean llevadas a cabo de forma omisiva asume, a nuestro parecer, una relevancia relativa, en la medida en que, como se detallará, los supuestos prototípicos de comisión por omisión concebibles en este ámbito pueden ser resueltos mediante la aplicación de otros preceptos del código penal. En realidad, únicamente resultan problemáticos cuando el sujeto que revela, difunde o cede la información deba ostentar unas especiales cualidades, esto es, en el tipo de injusto previsto en el art. 279.1 CP y, además, no se encuentre específicamente prevista la conducta caso de que ésta sea cometida por un no cualificado. No obstante, aunque de modo sucinto, se estima conveniente formular algunas consideraciones acerca de las diversas hipótesis que resultan proponibles en estos casos.

Las acciones típicas analizadas revisten la estructura de delitos de resultado —cifrado en la introducción del secreto en la esfera de disponibilidad del destinatario de la comunicación—, en los que no se han establecido unos medios comisivos legalmente determinados¹⁴⁵⁷. Esto es, se sanciona la difusión, revelación o cesión de un secreto, pero no la concreta forma de

¹⁴⁵⁶ Sobre las diversas consecuencias dogmáticas derivadas de las dos categorías de delitos de participación necesaria y sus consecuencias para la apreciación de las formas intentadas, vid. RODRÍGUEZ PUERTA, M.J., *El delito de cohecho...*, *op. cit.*, pp. 104-105.

¹⁴⁵⁷ Así, vid., por ejemplo, MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, *op. cit.*, p. 80, que considera que se trata de un delito puramente resultativo o CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 219.

acometimiento de las mismas –por medio de manifestación oral, por escrito, mediante el envío de correspondencia, de una copia, de un modelo o de una fotografía, a través de medios audiovisuales o informáticos, con entrega de soporte, etc.--. Además, el art. 279.1 CP incrimina la infracción de un especial deber jurídico, legal o contractual, de guardar reserva, como condición típica que debe reunir el sujeto activo del delito. Todo ello determina que sea necesario estudiar la posibilidad de que el art. 279.1 CP entre en el ámbito de proyección del art. 11 CP, que contiene la fórmula legal de la comisión por omisión¹⁴⁵⁸.

El principio de **equivalencia material** [«cuando la no evitación del mismo, (...), equivalga, (...), a su causación»], como criterio rector básico sobre el que se asienta la fórmula legal, reclama, además, como límite formal, que sea inferible una **equivalencia jurídica** o normativa, «según el sentido de la ley»¹⁴⁵⁹. Es decir, que se trate de verbos típicos compatibles gramaticalmente con la modalidad omisiva¹⁴⁶⁰. En el caso que se analiza –revelación cometida por un obligado a preservar el secreto, cuando éste no lleva a cabo la acción típica de forma directa, sino que se limita a no evitar que un tercero conozca la información empresarial--, en principio, se trata de acciones que admiten las formas omisivas, por lo que resulta predicable esta

¹⁴⁵⁸ Así, vid., entre otros, VIVES ANTÓN, T.S., “Comentario al artículo 11”, en VIVES ANTÓN, T.S. (Coord.), **Comentarios al Código Penal de 1995**, T. I, Valencia, 1996, pp. 85-86; MORALES PRATS, F., “Comentario al artículo 11”, en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código..., op. cit.**, 2ª. ed., p. 93 y SILVA SÁNCHEZ, J.M., **El nuevo Código penal: cinco cuestiones fundamentales**, Barcelona, 1997, p. 75.

¹⁴⁵⁹ Así, vid. VIVES ANTÓN, T.S., “Comentario al artículo 11”, en VIVES ANTÓN, T.S. (Coord.), **Comentarios al Código..., op. cit.**, pp. 85-86; MORALES PRATS, F., “Comentario al artículo 11”, en QUINTERO OLIVARES, (Dir.), **Comentarios al Nuevo Código..., op. cit.**, 2ª. ed., pp. 92-93 y SILVA SÁNCHEZ, J.M., **El nuevo Código penal: cinco..., op. cit.**, pp. 66-67.

¹⁴⁶⁰ En sentido contrario, vid. CARBONELL MATEU, J.C., en AA VV, **Derecho penal, Parte especial**, 2ª ed., Valencia, 1996, p. 473, que considera que se trata de verbos activos, sin que, por ello, quepa en la práctica la modalidad omisiva.

equivalencia jurídica¹⁴⁶¹. Así, se entiende que lleva a cabo estas conductas el sujeto que, intencionadamente, **no impide** que un tercero tome conocimiento del secreto, quebrantando la obligación jurídica de guardar reserva sobre los secretos que conoce como consecuencia de su situación en la empresa y que, expresa o concluyentemente, se le han confiado¹⁴⁶².

En resumen, pues, para que la modalidad omisiva de estas conductas sea punible será necesario que, junto a la presencia del deber jurídico de sigilo, pueda afirmarse un juicio de equivalencia valorativo-material y normativo-formal¹⁴⁶³.

Por lo que se refiere a estos delitos, quizá lo más conflictivo se cifre en constatar si existe o no un especial deber jurídico que genere esa necesaria posición de garante, es decir, si el mero conocimiento de la información como consecuencia de la situación que se ocupa en la empresa es capaz de provocar la especial situación de garante que debe vincular al sujeto activo¹⁴⁶⁴. Dado que no puede abundarse en este momento en el

¹⁴⁶¹ Por ejemplo, entre la conducta de dejar que otro acceda a un documento en el que consta el procedimiento de montaje de una nueva planta y la conducta de aportar una copia de tal procedimiento.

¹⁴⁶² Así, MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos, op. cit.*, p. 139; MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 80; MORALES PRATS, F./MORÓN LERMA, E., en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código..., op. cit.*, 2ª. ed., p. 1291; CARRASCO ANDRINO, M.M., en *La protección penal..., op. cit.*, p. 219; SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., *Comentarios al..., op. cit.*, p. 807; en sentido contrario, vid. CARBONELL MATEU, J.C., en AA VV, *Derecho penal, Parte especial, op. cit.*, p. 473.

¹⁴⁶³ Como criterios consagrados por el art. 11, vid., entre otros, VIVES ANTÓN, T.S., "Comentario al artículo 11", en VIVES ANTÓN, T.S. (Coord.), *Comentarios al Código..., op. cit.*, pp. 85-86; MORALES PRATS, F., "Comentario al artículo 11", en QUINTERO OLIVARES, (Dir.), *Comentarios al Nuevo Código..., op. cit.*, 2ª. ed., pp. 92 y ss. y SILVA SÁNCHEZ, J.M., *El nuevo Código penal: cinco..., op. cit.*, pp. 66-67; por lo que se refiere al art. 279.1 CP, vid. MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 80 y CARRASCO ANDRINO, M.M., en *La protección penal..., op. cit.*, p. 221.

¹⁴⁶⁴ Indudablemente, el contenido de la obligación de reserva puede variar de unos sujetos a otros. Así, por ejemplo, como acertadamente ejemplifica CARRASCO ANDRINO, M.M., en

particularizado análisis que esta cuestión reclama¹⁴⁶⁵, debe concluirse que, según advierte la doctrina, la equiparación automática del contrato como fuente del deber de garantía no se revela una solución satisfactoria¹⁴⁶⁶. En efecto, no parece que el mero deber de silencio derivado del contrato pueda fundamentar **per se** una posición de garante (art. 11 CP). Lógicamente, ello conduce a que sea preferible exigir una especial aceptación o compromiso por parte del sujeto obligado, lo que, a nuestro parecer, tampoco resulta una tarea de concreción jurídica sencilla. Al respecto, CARRASCO ANDRINO considera que esta obligación de guardar reserva aparece cuando «al sujeto le **han sido confiados** los secretos de la empresa, bien porque éstos constituyen el objeto de su contrato (el investigador, el licenciatario de know-how) o bien porque son la materia que le corresponde analizar para desarrollar las tareas propias de su trabajo (el inspector de trabajo, el administrador, el funcionario público, etc.)»¹⁴⁶⁷. Así, al confiarse el secreto, surge la necesaria relación de dependencia, que genera en el sujeto un deber de aseguramiento. Sin duda, se trata de un posicionamiento que, en la

La protección penal..., *op. cit.*, p. 221, no parece equiparable ni equivalente la obligación de reserva que pesa sobre un consejero-delegado o cualquier otro alto directivo de una empresa, al que se le confían los secretos de la misma, que la que le puede corresponder a un empleado administrativo o al personal de la limpieza, a los que no se les encomiendan tales secretos. Ello evidencia, en último término, la imposibilidad de admitir una equiparación automática del contrato como fuente del deber de garantía.

¹⁴⁶⁵ Sobre el tema, vid., ampliamente, CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, pp. 221 y ss. y PÉREZ DEL VALLE, C., “La revelación de secretos de empresa por persona obligada a reserva”, en **Delitos relativos a la propiedad industrial, al mercado y a los consumidores**, CDJ, CGPJ, 1997, pp. 113 y ss.

¹⁴⁶⁶ Así, vid. SILVA SÁNCHEZ, J.M., “Política criminal y reforma legislativa en la «comisión por omisión»”, en **Política Criminal y Reforma Legislativa, Homenaje al Prof. Dr. D. Juan del Rosal**, Madrid, 1993, p. 1077, que hace referencia a un actuar que implique un control sobre el riesgo equiparable al que se tiene por la vía de su creación activa; de igual modo, HUERTA TOCILDO, S., **Principales novedades de los delitos de omisión en el Código penal de 1995**, Valencia, 1997, p. 37, alude, para que se dé la equivalencia material, a la libre aceptación de una función de protección de un bien jurídico o de vigilancia de una fuente de peligro.

¹⁴⁶⁷ CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, p. 222.

medida en que resulta restrictivo del ámbito de la comisión por omisión, puede ser asumido.

Admitido lo anterior, esto es, la excepcionalidad de la atribución de una posición de garante al sujeto “custodio” del secreto, la problemática de la comisión por omisión en los delitos especiales, siendo un tema complejo, únicamente se presentará conflictivo cuando el comportamiento del sujeto a quien, omisivamente, se facilita la conducta ilícita (en este caso, el acceso ilícito a la información) no sea típico. Quizá en esos supuestos resulte conveniente acudir a la estructura de la comisión por omisión, dado que, al no haberse previsto específicamente una modalidad delictiva capaz de albergar esos comportamientos, la conducta podría quedar impune¹⁴⁶⁸.

Al margen de lo expuesto, pueden plantearse varios supuestos, cuya solución, como a continuación se aborda, es diversa.

I) Un consejero delegado, intencionadamente, deja sobre la mesa de la sala donde negocia información secreta sometida al deber de reserva.

II) Un director de producción, intencionadamente, deja al visitante en el área reservada donde se guarda la fórmula secreta, el plano de una moderna planta de montaje o el prototipo de una nueva maquinaria o le facilita las señas que le permiten llegar hasta allí¹⁴⁶⁹.

¹⁴⁶⁸ Aunque, quizá, en los casos en que la conducta del tercero no es típica, lo más adecuado resulte la previsión específica de una cláusula de equiparación o, según la terminología de SILVA, de una omisión pura de garante (así, vid. SILVA SÁNCHEZ, J.M., El delito de omisión. Concepto y sistema, Barcelona, 1986, pp. 343 y ss y, en especial, 347 y ss.). Así se ha hecho, por ejemplo, en la violación de secretos cometida por autoridad o funcionario público, prevista en art. 415 CP o en el delito de malversación, previsto en el art. 432 CP.

¹⁴⁶⁹ Así, vid., similarmente, SCHAFHEUTLE, K., *Wirtschaftsspionage und...*, op. cit., p. 93 y RAMELLA, A., “I segreti...”, en op. cit., p. 501, recogidos también por CARRASCO ANDRINO, M.M., en *La protección penal...*, op. cit., p. 220.

III) Un programador del departamento informático, intencionadamente, deja en pantalla la información en su despacho o facilita la clave de acceso.

IV) Un subdirector del departamento de marketing, intencionadamente, deja abierta la puerta de un recinto en el que se puede tener acceso a secretos comerciales o da la llave de su despacho en el que también se almacenan.

En estos supuestos, aunque por diversas vías, la conducta del tercero a quien es «revelada» la información es punible, con independencia de la aportación realizada por el obligado a guardar el secreto. En el caso del consejero delegado (primer supuesto), que deposita los documentos en un lugar accesible, se trata de una conducta activa de cesión o de revelación (art. 279.1 CP), aunque no se haya revelado directa e inmediatamente –como tampoco se hace cuando se envía por correspondencia una carta con un listado de proveedores--.

En todos los demás casos (segundo, tercer y cuarto supuestos), la conducta del director, del programador y del subdirector deben ser calificadas de **participación**. Como se ha señalado, en estos supuestos no se hallan obstáculos para sancionar al partícipe, puesto que la conducta del autor es típica, de modo que, en los tres últimos ejemplos, el tercero a quien se revela **comete activamente** el delito previsto en el art. 278.1 CP, que castiga el acceso ilícito a la información y el obligado que facilita la realización de esta acción típica, **participa activamente** en dicho acceso, siempre que se cumplan el resto de requisitos típicos¹⁴⁷⁰. Evidentemente,

¹⁴⁷⁰ En diverso sentido, CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 222, alude a la posibilidad de pensar, en estos casos, «en una **participación omisiva** en el delito de comisión de un tercero» (la cursiva es mía). A nuestro parecer, en estos casos, la participación es precisamente activa. El sujeto obligado lleva a cabo actos positivos (facilitar

además de éstos, deberá constatarse asimismo un acuerdo de voluntades, entre el sujeto obligado y el que accede al secreto¹⁴⁷¹. De no concurrir tal circunstancia, la conducta del custodio del secreto sería impune, puesto que la revelación imprudente es atípica, mientras que la acción llevada a cabo por el tercero que accede a los documentos aprovechando el descuido de otro, deberá subsumirse en la modalidad delictiva prevista en el art. 278.1 CP.

A favor de la solución formulada abogan varias razones. En primer lugar, la posibilidad de sancionar a todos los sujetos que intervienen en el hecho delictivo. Así, con arreglo a dicha propuesta, la conducta del sujeto a quien se ha permitido el acceso a la información será calificada de autoría, por medios comisivos, de un delito previsto en el art. 278. 1 CP y la conducta del sujeto que facilita el acceso será una conducta de participación.

Por el contrario, la resolución será distinta y, a nuestro parecer, menos adecuada, si se hace responder al obligado por un delito de revelación del art. 279.1 CP, en comisión por omisión, puesto que, en ese caso, únicamente resultará punible su conducta y no la del tercero que, en los ejemplos sugeridos, se limita a ser la de recepción del secreto, comportamiento que sólo podrá ser sancionado si la usa en provecho propio o la vuelve a revelar, en cuyo caso vendrá en aplicación el art. 280 CP.

Por otra parte, la valoración jurídica de las diversas conductas que ha previsto el legislador también debe aprehender los diversos perfiles y

la clave del ordenador, dejar la puerta abierta o los documentos en pantalla, conducir a alguien a un recinto reservado).

¹⁴⁷¹ Así, vid. HUERTA TOCILDO, S., *Problemas fundamentales de los delitos de omisión*, Madrid, 1987, p. 249 y CARRASCO ANDRINO, M.M., en *La protección penal...*, op. cit., p. 222.

matices que las mismas asumen. En esta medida, no resulta equiparable la conducta de quien escucha o se limita a recibir pasivamente la información que le es comunicada activamente por un sujeto, que la de aquel tercero que lleva a cabo acciones positivas tendentes a obtener esa información, como pueden ser la de abrir la puerta del recinto reservado o del despacho, acceder al mismo y mirar la información en pantalla, introducir la clave en el ordenador, etc. La diferente entidad que, valorativamente, revisten estos comportamientos debe ser, asimismo, aprehendida jurídicamente, sobre todo, en la medida en que el legislador ha previsto vías diversas para captar estos matices.

Además, desde la perspectiva de la penalidad, la solución por la que aquí se ha optado permite imponer una sanción adecuada a la gravedad del ilícito, tanto a uno como a otro sujeto, puesto que la pena que corresponde al sujeto obligado puede incluso llegar a ser superior si responde como partícipe en un acceso ilícito con posterior revelación (participación en el delito previsto en el art. 278.2 CP). O, en todo caso, igual a la que le correspondería si su conducta fuera calificada de autoría en un delito de revelación (art. 279.1 CP).

En cualquier caso, la propuesta formulada alzaprima la valoración de la acción frente a las posibles omisiones. En todos los supuestos planteados, el obligado, en primer lugar, ejecuta una conducta positiva, previa o simultánea a las acciones omisivas. En esta medida, y según viene siendo admitido, debe, en primer término, acometerse la calificación del hecho tomando en consideración su posible subsunción como comportamiento positivo y sólo en el caso de que esto resulte infructuoso, debe procederse a su calificación como conducta omisiva.

En conclusión, pues, la solución propugnada no hace necesario forzar la posición de garante, ni la equivalencia valorativo-material. Antes bien, permite aprehender la diferente entidad de conductas pasivas u omisivas y de comportamientos positivos, susceptibles de ser valorados jurídico-penalmente. Así, dejar los documentos en una mesa donde se negocia es constitutivo de la conducta típica de cesión; facilitar la clave de acceso a un ordenador donde se halla la información no integra una conducta de revelación, sino de participación en un acceso ilícito. Por otra parte, desde la perspectiva del destinatario de la comunicación, tampoco resulta equiparable valorativamente, la conducta de quien, simplemente, se limita a escuchar a la de quien abre la puerta de un recinto reservado, busca la información y accede a ella o la de quien introduce la clave de acceso en un ordenador y accede a la información.

V. «Utilización».

1. Concepto de «utilización».

La última de las modalidades atentatorias estriba en la utilización del secreto. Se trata de una conducta específicamente contemplada en el código, aunque, como se expondrá, tampoco su previsión se halla exenta de problemas y contradicciones¹⁴⁷².

¹⁴⁷² La utilización del secreto se halla prevista en el artículo 279.2 CP e integra uno de los comportamientos recogidos en el art. 280 CP. El artículo 279.2 CP establece que: «Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior». El artículo 280 CP declara que: «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 su significado más corriente o coloquial, utilizar significa «aprovecharse de una cosa»¹⁴⁷³, «servirse de una cosa para algún fin útil»; a su vez, por útil debe entenderse «que produce o procura algún provecho, conveniencia o ventaja»¹⁴⁷⁴ y provecho equivale a «utilidad o beneficio que se origina de una cosa o por algún medio»¹⁴⁷⁵.

Por tanto, con arreglo a una interpretación estrictamente gramatical, la utilización de la información constituye un comportamiento cuyo significado presenta una extraordinaria amplitud, que comprende, en último término, cualquier uso de que sea objeto la información¹⁴⁷⁶. En esta medida, la utilización se configuraría como un concepto omnicomprendivo en el que quedarían incluidas las conductas de revelación, difusión y cesión.

Sin embargo, esta interpretación fagocita la previsión de las modalidades típicas anteriormente analizadas y conduce al solapamiento valorativo-material y jurídico de conductas de diversa entidad y significación. Así, resulta concebible, por ejemplo, que un sujeto revele una información bursátil, sin que lleve a cabo el aprovechamiento o explotación de la misma y, de igual modo, que un ex empleado pueda utilizar un listado de clientes en la nueva empresa que ha decidido crear, sin que se lleve a cabo su divulgación.

¹⁴⁷³ Real Academia Española, *Diccionario de la lengua española*, 21 ed., Madrid, 1992.

¹⁴⁷⁴ CASARES, J., *Diccionario ideológico de la lengua española*, 2 ed., Barcelona, 1971.

¹⁴⁷⁵ Real Academia Española, *Diccionario de la lengua española*, 21 ed., Madrid, 1992; segunda acepción.

¹⁴⁷⁶ En igual sentido, vid. GALÁN CORONA, E., "El Acuerdo ADPIC (TRIPS) y la protección de la información confidencial", en *Los acuerdos ADPIC (TRIPS), TLT y Protocolo del Arreglo de Madrid y su incidencia en la legislación española, Jornada de Estudio organizada por el GE de la AIPPI*, Barcelona, 1998, p. 98.

A nuestro parecer, pues, se trata de conductas con un desvalor material distinto, pero que pueden revestir análoga gravedad. Así, son imaginables supuestos en los que se produzca una divulgación extraordinariamente grave, desde la afección al bien jurídico y casos en que la utilización no resulte tan lesiva y, también, al contrario. Por ejemplo, si un ex empleado decide revelar la fórmula de la coca-cola y para ello convoca una rueda de prensa y comunica la información, dicha revelación comporta la total cercenación del bien jurídico. En cambio, si alguien, que conoce la relación de proveedores de una empresa textil, decide utilizarlo en la empresa que crea por su propia cuenta, quizá la peligrosidad que dicha conducta puede entrañar para el bien jurídico sea menor que en el caso anterior. Sin embargo, también son imaginables supuestos de revelaciones menos graves y de explotaciones más dañosas. Así, por ejemplo, la revelación de un listado de clientes a otro competidor puede constituir una conducta de menor lesividad. Y, por el contrario, la utilización de los modelos de una colección de ropa del competidor de la próxima temporada puede suponer una puesta en peligro o lesión más grave para el bien jurídico.

Así pues, aunque desde la perspectiva del bien jurídico no parezca posible arbitrar *a priori* una gradación lesiva entre ambas conductas¹⁴⁷⁷, sí deviene necesario mantener su distinción como modalidades atentatorias del secreto. De ahí que sea imprescindible acudir a una interpretación más restrictiva de la utilización, en cuya virtud se dote de ámbito propio a cada modalidad.

¹⁴⁷⁷ De otra opinión se muestra TERRADILLOS BASOCO, J., *Derecho penal...*, *op. cit.*, p. 173, quien considera que la utilización «recorta menos la capacidad competitiva de la empresa en el mercado que la difusión indeterminada»; en sentido análogo, MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, *op. cit.*, p. 85, manifiesta que «el radio de la acción peligrosa (y consecuentemente la potencialidad lesiva de la conducta) es *a priori* mayor en la figura del tipo básico (revelación), al estar indeterminada la frontera del peligro que en la del tipo atenuado (utilización)»; de igual modo, ROBLEDOS VILLAR, A., *Delitos contra el patrimonio...*, *op. cit.* pp. 382-383, afirma la «menor entidad del peligro que para el bien jurídico protegido supone la utilización de la información reservada por persona que legal o contractualmente conocía la información utilizada».

Constatada, pues, la conveniencia de distinguir ambas acciones y de no unificarlas en un concepto común y más genérico, encarnado en la modalidad de uso, debe procederse a su delimitación. Al efecto, según se ha analizado ya, la conducta de revelación se integra por la transmisión del secreto fuera del círculo de los sujetos autorizados a conocerlo. Por el contrario, la utilización del secreto equivale, en cierta forma, a la realización o ejecución del secreto.

Profundizando en la exégesis de esta modalidad típica, una interpretación teleológica de la misma reclama, en primer lugar, vincular el uso del secreto al ámbito de la **competencia económica**. Es decir, «utilizar» supondrá el empleo del secreto en el marco del ejercicio de una actividad económica en el mercado, de modo que el uso que se dé a la información resulte objetivamente idóneo para obtener un disfrute o una ventaja competitiva, que suele derivar del secreto¹⁴⁷⁸. En suma, la utilización implicará **un aprovechamiento económico del secreto**.

En virtud de lo anterior, la conducta de utilización del secreto reviste una significación autónoma, en la que asume una relevancia determinante la tutela de la **situación de exclusividad en la disponibilidad de la información** y que, por tanto, resulta susceptible de ser desgajada como figura típica de las modalidades típicas de difusión, revelación y cesión.

El deslinde conceptual de ambas modalidades atentatorias permite, así, afrontar uno de los supuestos que suele presentarse especialmente problemático. Se trata de aquellos casos en los que el sujeto activo, habiendo accedido lícitamente al secreto, decide emplearlo posteriormente

¹⁴⁷⁸ Análogamente, vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 258.

en provecho propio al constituir su propia empresa, y para la ejecución o aprovechamiento del secreto debe llevar a cabo una revelación del mismo a sus propios empleados; o bien, debe comunicarlo a aquellos otros empresarios competidores con los que toma contacto y para quienes decide trabajar explotando el secreto; o debe revelarlo a otros terceros con los que decide asociarse, y en cuya vinculación quizá ha sido decisivo los secretos que el sujeto activo aporta.

En estos supuestos, la doctrina ha considerado que cuando la utilización del secreto (modalidad que se halla prevista en el art. 279.2 CP) exige inexcusablemente la transmisión del mismo a otras personas (prevista en el art. 279.1 CP), existe un concurso de normas en el que prevalece el tipo relativo a la difusión (art. 279.1 CP)¹⁴⁷⁹. En esta línea, que presupone equiparar o solapar el ámbito de ambas modalidades típicas, se ha denunciado que, con arreglo a la regulación vigente, podría suscitarse el siguiente dislate valorativo¹⁴⁸⁰, el ex empleado que, constituido en empresario, revela a sus nuevos trabajadores secretos empresariales pertenecientes a su antiguo empleador con el objeto de poner en marcha un nuevo proceso de fabricación o una nueva planta de montaje afronta una pena menor (art. 279.2 CP) que el que lo hace por despecho (art. 279.1 CP).

¹⁴⁷⁹ Así, vid. MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 87 y PÉREZ DEL VALLE, C., “La revelación de secretos de empresa por persona obligada a reserva”, en *Delitos relativos a la propiedad industrial, al mercado y a los consumidores*, CDJ, CGPJ, 1997, p. 138. En esta línea se halla la calificación del ejemplo propuesto por QUERALT -- relativo al sujeto que obligado a guardar reserva de un secreto de la empresa para la que trabaja es contratado por los responsables de la empresa competidora con el fin de que aquél transmita a éstos la información reservada--, analizado anteriormente por MARTÍNEZ-BUJÁN; así, vid. supra epígrafe relativo la caracterización de las modalidades de revelación, difusión y cesión como delitos de participación necesaria.

¹⁴⁸⁰ Así es denunciado por MASSAGUER FUENTES, J.J., “Los secretos industriales y comerciales...”, en FONT GALÁN, J.I./NAVARRO CHINCHILLA, J.J./VÁZQUEZ GARCÍA, R.J., *Derecho de la..., op. cit.*, p. 184.

Sin embargo, al margen de dislates valorativos desde la perspectiva de la penalidad a los que posteriormente se hará referencia, a tenor de la delimitación típica postulada, no parece compartible la calificación de los hechos. No se nos oculta que, en la actualidad, gran parte de los secretos empresariales, por su propia idiosincrasia, requieren para poder ser ejecutados en los sistemas o procesos de producción, una revelación previa del mismo, cuando menos, a los propios empleados para proceder a su explotación. Hoy en día, la información de la que disponen las empresas para ganar cuota de mercado y mantener o incrementar, así, su posición competitiva, no se cifra en informaciones susceptibles de ser explotadas unilateralmente, como podía ocurrir en la sociedad artesanal de la Edad Media. De ahí que, a nuestro parecer, esta revelación sea consustancial, en estos casos, a la conducta de utilización, dado el grado de desarrollo técnico y la complejidad de la información de la sociedad moderna¹⁴⁸¹.

Esto no significa que en aquellos casos, en los que la conducta llevada a cabo por el sujeto consista en un previa revelación del secreto para poder ser explotado por terceros, no deba calificarse o subsumirse la conducta en la modalidad de revelación del art. 279.1 CP. A nuestro parecer, no puede equipararse el caso antes mencionado (revelación a los trabajadores para que ejecuten) con el supuesto en que un sujeto revela por precio el secreto a un competidor para que éste lo explote (en esta hipótesis, el sujeto respondería como autor del art. 279.1 CP y el competidor a través del art. 280 CP) o con aquel otro en que el sujeto obligado a mantener la reserva es contratado por una empresa competidora precisamente para que ponga en su conocimiento el secreto del que dispone y poder, así, explotarlo

¹⁴⁸¹ GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), **Curso de derecho penal, op. cit.**, p. 802, considera ceñido el ámbito de la modalidad de utilización prevista en el art. 279.2 CP, a los supuestos en los que no hay difusión, revelación o transmisión del secreto. Sin embargo, no se alcanza a comprender si está haciendo referencia a una delimitación del ámbito típico de cada modalidad o bien a la restricción del art. 279.2 CP a los supuestos en que no se produzca la revelación del secreto a ningún tercero.

(el sujeto obligado sería autor del art. 279.1 CP y los competidores del art. 280 CP). En ambos casos, pese a existir un uso del secreto, éste tiene su origen en una revelación ilícita, con sustantividad propia desde una perspectiva empírica y jurídica. Es el primer paso ilícito en esa concatenación de acciones también ilícitas.

En una hipótesis de delimitación de supuestos, cada una de estas acciones asume su propio ámbito operativo. Si el paradigma de la revelación se sitúa en aquellos casos en los que el depositario de la información la comunica a una o a varias personas (con independencia del posterior uso que éstas hagan de ella), los supuestos prototípicos de utilización podrían residir en aquellos en los que el obligado a mantener la reserva se constituye en empresario, aprovechando para sí el secreto de empresa o en aquellos otros en los que el sujeto se asocia con un tercero –como socio capitalista, por ejemplo—y explota económicamente el secreto.

En estos dos últimos supuestos, aunque evidentemente se requiere llevar a cabo una revelación, ésta pierde importancia frente al prioritario uso del secreto que busca el autor del delito¹⁴⁸².

Así pues, admitida la entidad de la utilización como **modalidad atentatoria de carácter autónomo**, como lo es el acceso a los secretos o su divulgación, en la progresiva delimitación de su ámbito, esta acción comprende la **utilización** o los usos **del secreto al que se ha podido acceder abusiva o ilícitamente**, la **utilización del secreto al que se ha podido acceder lícitamente** y la **utilización o uso del secreto, por parte del tercero al que se le ha revelado** y que, por tanto, lo conoce en virtud de un hecho ilícito.

¹⁴⁸² Penalidad: remitir a lo de la falta a la vida: arts. 278.1 y 278.2

En conclusión, pues, desde una perspectiva **de lege lata**, debe formularse una interpretación atenta a los diversos matices y perfiles que ambas acciones presentan (revelación y utilización), lo que determina el rechazo de una interpretación amplia del término «utilizar». De otro lado y desde una perspectiva **de lege ferenda**, sería conveniente, una vez reconocida su autonomía como modalidad atentatoria del secreto, concretar mejor la acción y, a tal objeto, emplear un vocablo menos polisémico, que evite consecuencias interpretativas disfuncionales. En este sentido, podría acudirse al término adoptado por el art 13 LCD¹⁴⁸³, «explotar», que parece evocar más directamente el aprovechamiento económico o la obtención de alguna ventaja competitiva que caracteriza esta acción típica¹⁴⁸⁴.

2. El elemento subjetivo como criterio delimitador del ámbito típico.

En la definición de lo que constituye el ámbito de lo punible a partir del análisis de las acciones típicas, por lo que atañe a la utilización –al igual que ocurría en las modalidades de acceso-- es necesario acudir al elemento subjetivo, puesto que la parte objetiva del tipo queda trazada en función de aquél. De modo que, en la determinación de qué constituye **utilización o explotación típica**, deviene indispensable la función restrictiva que ejerce el elemento subjetivo del injusto.

Así pues, la explotación, además de con finalidad de aprovechamiento económico, reclama ser precisada a través del elemento subjetivo. De

¹⁴⁸³ En el derecho comparado, la UWG alemana, en el § 17, (2), 2, emplea el término **verwertet** y el CPI, en el art. 623, acude a **impiegare**. Ambos equivalen al vocablo español «utilizar».

¹⁴⁸⁴ En similar sentido, vid. GALÁN CORONA, E., “El Acuerdo ADPIC (TRIPS) y la protección de la información confidencial”, en **Los acuerdos ADPIC (TRIPS), TLT y Protocolo del Arreglo de Madrid y...**, op. cit., p. 98.

hecho, el propio código penal, en el artículo 279.2, emplea la expresión «**en provecho propio**».

Sin duda, este elemento --en provecho propio-- incide en el contenido que asume el verbo utilizar y se convierte, por tanto, en una pieza indispensable para lograr una significación jurídica de la conducta típica.

Ahora bien, especialmente dividida se muestra la doctrina en la determinación de la naturaleza jurídica de este elemento. Siguiendo las posiciones mantenidas en la literatura italiana, el elemento del provecho propio, puede ser entendido de tres modos diversos¹⁴⁸⁵; en primer lugar, como un componente **de índole subjetiva**, que preside la conducta de utilización del sujeto activo con una específica finalidad¹⁴⁸⁶; en segundo término, con un contenido de cariz objetivo, como la obtención de un beneficio por parte del sujeto, conectado causalmente al empleo o disfrute del secreto¹⁴⁸⁷; y, por último, a modo de solución intermedia, como elemento también de tenor objetivo relativo a la conducta, que alude a la necesidad de que la utilización sea efectivamente idónea para otorgar una ventaja al agente y, por tanto, para causar un perjuicio al titular del secreto, para que devenga una utilización típica¹⁴⁸⁸.

¹⁴⁸⁵ El art. 623 CPI establece que: «Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni».

¹⁴⁸⁶ CRESPI, A., "Tutela penale...", en *op. cit.*, p. 185.

¹⁴⁸⁷ MAZZACUVA, N., *La tutela penale*, p. 121, n. 25.

¹⁴⁸⁸ ALESSANDRI, A., *Riflessi penalistici della ...*, *op. cit.*, p. 269.

Análogamente, en nuestra doctrina¹⁴⁸⁹, una de las posturas sostenidas configura el provecho propio como parte integrante del resultado típico de la conducta, de modo que se concibe el tipo del art. 279.2 CP como un delito de resultado material¹⁴⁹⁰, cuyo contenido se conforma «por el provecho que al propio autor le reporta indefectiblemente la utilización del resultado»¹⁴⁹¹.

Ciertamente, como afirma MARTÍNEZ-BUJÁN¹⁴⁹², la obtención de tal provecho no debe ser entendida automáticamente como reveladora de la producción de un resultado lesivo¹⁴⁹³, puesto que la utilización en provecho propio posee idoneidad lesiva para poner en peligro el interés económico del empresario, pero no presupone necesariamente la lesión efectiva de dicho interés. Ello es fundamentalmente así, puesto que la utilización del secreto en provecho propio conlleva, con arreglo a una interpretación gramatical del mismo, de forma inherente, la obtención del provecho. Pero, según una interpretación teleológica, la utilización del secreto en provecho propio debe ceñirse al aprovechamiento económico, esto es, a aquellos usos que resulten idóneos para ser explotados o empleados en el ejercicio de una actividad económica, por resultar susceptibles de proporcionar una ventaja competitiva. En esa medida, la **utilización del secreto será típica sólo cuando sea llevada a cabo para obtener una ventaja competitiva que redunde en el propio beneficio**. Y ésta significación normativo-teleológica de la utilización

¹⁴⁸⁹ Sobre los posicionamientos doctrinales sostenidos respecto del elemento «en perjuicio de tercero» del art. 499 ACP, vid. supra, en la primera parte, capítulo II, epígrafe 2.2.2., relativo al interés en el mantenimiento del secreto.

¹⁴⁹⁰ Así, vid. JORDANA DE POZAS GONZÁLBEZ, L., en CONDE-PUMPIDO FERRERIO, C. (Dir.), *Código penal, doctrina y jurisprudencia*, T. II; Madrid, 1997, p. 2981.

¹⁴⁹¹ MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, p. 84.

¹⁴⁹² MARTÍNEZ-BUJÁN PÉREZ, C., *ibidem*.

¹⁴⁹³ Así parece entenderlo por CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 261.

es la que, a nuestro parecer, justifica que el citado elemento deba ser entendido con un contenido subjetivo, que colorea y preside la ejecución de la conducta del sujeto activo.

Así, a nuestro juicio, la expresión «en provecho propio» constituye un **elemento subjetivo del injusto**¹⁴⁹⁴, que convierte al tipo en un delito de tendencia interna trascendente¹⁴⁹⁵, en cuya virtud basta que el sujeto emplee el secreto guiado por el ánimo de obtener una ventaja o beneficio a su favor para que se consume, siendo irrelevante a dichos efectos su agotamiento o acaecimiento efectivo.

En cuanto al significado que, propiamente, ostenta la cláusula «en provecho propio», de nuevo será necesario acudir al bien jurídico, que, en su función exegética, oriente, asimismo, la de dicho elemento. El provecho sólo puede comprender las ventajas o beneficios vinculados al ejercicio de una actividad económica y, por tanto, debe asumir necesariamente un contenido económico¹⁴⁹⁶, de forma que pueda entenderse como una utilidad confluyente con la protegida por el secreto¹⁴⁹⁷. Sólo así puede concebirse

¹⁴⁹⁴ En igual sentido, vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, *op. cit.*, p. 261; MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos*, *op. cit.*, p. 141 y ROBLEDÓ VILLAR, A., *Delitos contra el patrimonio...*, *op. cit.* p. 383; en contra, vid. MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, *op. cit.*, p. 84 y GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal*, *op. cit.*, p. 802.

¹⁴⁹⁵ Acerca de la caracterización de estos delitos, también denominados «delitos de intención», vid., en nuestra doctrina, entre otros, OCTAVIO DE TOLEDO Y UBIETO, E./HUERTA TOCILDO, S., *Derecho penal, Parte general*, *op. cit.*, p. 137; MIR PUIG, S., *Derecho penal, Parte general*, *op. cit.*, p. 205; LUZÓN PEÑA, D.M., *Curso de derecho penal, Parte general*, *op. cit.*, pp. 316-317 y, en derecho comparado, vid. JESCHECK, H.H., *Tratado de Derecho Penal, Parte General*, *op. cit.*, vol. I. pp. 436-437 y ROXIN, C., *Derecho penal, Parte general*, *op. cit.*, p. 317.

¹⁴⁹⁶ En contra, vid. GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal*, *op. cit.*, p. 802, que considera que «el provecho propio no tiene por qué ser necesariamente de naturaleza económica».

¹⁴⁹⁷ Así, vid. MAZZACUVA, N., *La tutela penale*, p. 122, n. 27; ALESSANDRI, A., *Riflessi penalistici della ...*, *op. cit.*, pp. 270-271; COCCO, G., «La tutela penale del segreto

como una conducta idónea para entrar en conflicto y poner en peligro el interés económico del empresario¹⁴⁹⁸.

Por tanto, deben desecharse como conductas subsumibles en esta modalidad las utilidades llevadas a cabo para obtener cualquier otro tipo de provecho, como puede ser el de carácter moral, personal o ideológico¹⁴⁹⁹. Así, no será típica la conducta del sujeto obligado a guardar reserva que se aprovecha del conocimiento del secreto para conseguir un puesto de trabajo para un amigo¹⁵⁰⁰. Tampoco la utilización de un procedimiento de montaje para profundizar en su conocimiento por puro deseo de aprendizaje deviene una conducta ilícita¹⁵⁰¹. Y, de igual modo, la utilización de cualquier secreto con el fin de conseguir incrementar la reputación o la fama comercial será punible en la medida en que la persecución de dicho renombre revierta en un deseo de aprovechamiento económico¹⁵⁰².

Así, quedan al margen de esta modalidad comisiva –tanto respecto del tipo previsto en el art. 279.1 como en el art. 280 CP-- las acciones

industrial", en DI AMATO, A., *Tratato di Diritto Penale...*, op. cit., p. 301 y MUTTI, P., "Segreti scientifici o industriali (rivelazione di)", en *Digesto delle Discipline Penalistiche*, vol. XIII, UTET, Torino, 1997, p. 79.

¹⁴⁹⁸ En igual sentido, vid. CARRASCO ANDRINO, M.M., en *La protección penal...*, op. cit., p. 262.

¹⁴⁹⁹ Análogamente, vid. COCCO, G., "La tutela penale del segreto industriale", en DI AMATO, A., *Tratato di Diritto Penale...*, op. cit., p. 301 y MUTTI, P., "Segreti scientifici...", en *Digesto...*, op. cit., p. 79.

¹⁵⁰⁰ Así, vid. MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, op. cit., p. 86.

¹⁵⁰¹ Así, CARRASCO ANDRINO, M.M., *ibidem*.

¹⁵⁰² En contra, vid. MARCHENA GÓMEZ, M., en SERRANO BUTRAGUEÑO, I., Coord., *Código penal de 1995 (Comentarios y jurisprudencia)*, Granada, 1998, p. 1371, que considera que no son excluibles otras formas de provecho, como, por ejemplo, la reputación en los mercados, que no se orienten de forma exclusiva y primaria al rendimiento económico.

acometidas en provecho ajeno o con ánimo de perjudicar al titular del secreto¹⁵⁰³.

Por lo que se refiere **al provecho ajeno**, ciertamente, en la mayor parte de ocasiones el sujeto que, conociendo lícitamente el secreto --o fruto de una revelación ilícita--, decide utilizarlo, suele hacerlo de diversas formas. Una de ellas radica en crear su propia empresa que entra en competencia con la del agente para el que trabajaba (su antiguo empleador); otra, vinculándose o asociándose a uno o varios terceros --como socios capitalistas--. Y, en esa medida, dado que **la utilización en provecho propio no debe ser equiparada con la utilización en provecho exclusivo del agente**, los supuestos en que el beneficio puede llegar a ser compartido, por ejemplo, a través de los socios, resultan también subsumibles en esta modalidad de acción típica, aunque no se haya previsto de forma expresa el elemento del provecho ajeno¹⁵⁰⁴. Ahora bien, no se agotan ahí los casos en que la utilización puede acometerse sin perseguir un resultado ventajoso para el sujeto activo. Así, por ejemplo, el sujeto que utiliza el secreto, nominalmente por cuenta propia, pero que, en realidad, lo hace para provecho ajeno, como prestanombre (a modo de testaferro) o como instrumento de un tercero competidor¹⁵⁰⁵. De ahí que, aun siendo un extremo complejo, quizá convenga reflexionar acerca de la posibilidad, **de lege ferenda**, de introducir junto al elemento del provecho propio el del provecho ajeno¹⁵⁰⁶. A nuestro parecer, en la utilización del secreto lo

¹⁵⁰³ Por el contrario, estos ánimos son específicamente contemplados en la LCD española y en la UWG alemana.

¹⁵⁰⁴ Vid., en igual sentido, CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, p. 259.

¹⁵⁰⁵ RAMELLA, A., "I segreti...", en *op. cit.*, p. 502.

¹⁵⁰⁶ En contra, vid. CARRASCO ANDRINO, M.M., en **La protección penal...**, *op. cit.*, pp. 258-259. Tampoco parece partidario de su introducción MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte especial**, *op. cit.*, p. 86, que considera poco probables las utilidades del secreto en provecho ajeno, siempre que tales utilidades no entrañen al

relevante es que asuma contenido económico, independientemente de que el sujeto activo persiga la ventaja en beneficio propio o ajeno, aunque, desde una perspectiva criminológica, lo habitual sea que se emplee para provecho propio.

En cuanto ***al ánimo de perjudicar al titular del secreto***, lo cierto es que resulta complejo imaginar un caso de utilización del secreto para causar un daño a su poseedor en el que no subyazca conjuntamente el ánimo de obtener un provecho propio o ajeno. Aun admitida esta dificultad, podría darse el supuesto en que un sujeto decide utilizar el secreto, produciendo a precio inferior al coste, para hundir al competidor, generándose, pongamos por caso, una situación monopolística¹⁵⁰⁷. Así, aunque, ***a priori***, su previsión ***de lege ferenda*** no se revele una cuestión de relevancia similar a la del elemento anterior cifrado en el provecho ajeno, no obstante, parece aconsejable postular también su incorporación.

En conclusión, pues, a nuestro parecer, análogamente a la fórmula propuesta en la modalidad de apoderamiento, la definición de lo punible recama la presencia de un elemento de cariz subjetivo de contornos más

propio tiempo una difusión, revelación o cesión del secreto a esas otras personas, en cuyo caso, según el citado autor, dichas conductas —de utilización en provecho ajeno—integrarían el tipo básico (art. 279.1 CP). Desde luego, ***de lege lata***, resulta compatible esta interpretación, en la medida en que permite solventar una indeseable laguna legal y siempre que no sea un supuesto de provecho compartido. Pero no como posicionamiento o propuesta ***de lege ferenda***, puesto que, según se ha indicado, la utilización y la revelación constituyen modalidades típicas diversas, que reclaman ámbitos también distintos, en cuya configuración, precisamente, el elemento subjetivo asume una relevancia de desigual entidad. En el caso de la explotación, la presencia del componente de índole subjetiva deviene imprescindible, a diferencia de lo que ocurre en la revelación, difusión o cesión, cuya lesividad objetiva queda trazada ya a partir del dolo del delito.

¹⁵⁰⁷ Sin duda, se trata de una hipótesis de laboratorio, que, supone, además, partir de un determinado sector de mercado, en el que la oferta del producto se halle concentrada en pocas manos. Así, por ejemplo, en piezas destinadas al sector siderúrgico de difícil fabricación; chips; software. Sin que se trate de un supuesto análogo, podría pensarse, pongamos por caso, en el caso de Microsoft que, regala junto al software que produce, un navegador, resultando perjudicados el resto de competidores del ramo, que comercializan otros navegadores.

amplios, en cuya virtud se seleccionen las conductas con capacidad de afección sobre el bien jurídico, aunque suponga, en cierta medida, un adelantamiento de la tutela penal. Al efecto, según se ha sugerido ya¹⁵⁰⁸, se estima adecuada la opción prevista por la LCD española, que prevé como uno de los criterios determinantes de la explotación ilícita de los secretos que sea llevada a cabo con ***el ánimo de obtener provecho, propio o de un tercero o de perjudicar al titular del secreto***. El criterio adicional cifrado en el ánimo de competir —que contiene, por ejemplo, la UWG alemana—, se revela, en cambio, superfluo e innecesario¹⁵⁰⁹. Y, por el contrario, la restricción de la fórmula al provecho propio o ajeno —opción adoptada por el código penal italiano—deviene insuficiente¹⁵¹⁰.

Una vez analizado el concepto de la acción y definido el ámbito de lo punible a partir del elemento subjetivo propuesto, debe ya analizarse cuál es la significación que, ***de lege lata***, ostenta esta modalidad típica y cuál es la que, desde su afección al bien jurídico protegido, le corresponde asumir.

3. La «explotación del secreto» como modalidad comisiva que demanda autonomía propia.

La utilización o explotación del secreto se encuentra contemplada en el artículo 279.2 CP y, probablemente, constituye una de las modalidades de acción que más polémica ha suscitado, quizá, porque la técnica legislativa empleada en el código, que no resulta la más adecuada, genera confusión.

¹⁵⁰⁸ Vid., sobre el particular, supra epígrafe 2.1.2. relativo al elemento subjetivo como criterio delimitador del alcance de la modalidad típica de apoderamiento.

¹⁵⁰⁹ Vid., al respecto, supra epígrafe 2.1.2.

¹⁵¹⁰ El artículo 623 CPI sanciona únicamente la utilización en provecho propio o ajeno.

En la doctrina se han mantenido dos interpretaciones contrapuestas acerca de la naturaleza de esta modalidad típica prevista en el art. 279.2 CP. Así, mayoritariamente se considera que encarna una **modalidad atentatoria privilegiada**, respecto de la modalidad básica prevista en el art. 279.1 CP¹⁵¹¹ y, por el contrario, un sector minoritario la califica como **tipo autónomo**¹⁵¹².

Así pues, esta disparidad justifica que, aunque sucintamente, se planteen algunas de las objeciones y ventajas que dichas posiciones comportan, al objeto de poder asumir, argumentadamente, una de ellas.

I) La utilización del secreto, como modalidad de ataque atenuada.

Con arreglo a esta interpretación, la utilización del secreto se configura como una conducta típica dependiente de otra. Así pues, según la regulación de estas modalidades en el código, el tipo relativo a la utilización

¹⁵¹¹ Ésta es, en efecto, la postura que mayoritariamente asume la doctrina; así, vid. TERRADILLOS BASOCO, J., *Derecho penal...*, op. cit., p. 173, respecto del art. 274.2 PCP 1994; MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial*, op. cit., pp. 82 y ss.; GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal*, op. cit., p. 802; SUÁREZ GONZÁLEZ, C., en RODRÍGUEZ MOURULLO, G., Dir., *Comentarios al...*, op. cit., p. 808; MORENO CÁNOVAS, A./RUIZ MARCO, F., *Delitos socioeconómicos*, op. cit., p. 140; PRATS CANUT, J.M., "Descubrimiento y revelación de secretos...", en *Delitos relativos a la propiedad...*, op. cit., p. 200; PÉREZ DEL VALLE, C., "La revelación de secretos de empresa...", en *Delitos relativos a...*, op. cit., p. 123; FERNÁNDEZ SÁNCHEZ, M.T., *Protección penal...*, op. cit., pp. 313 y ss.; MUÑOZ CONDE, F., *Derecho penal, Parte Especial*, 11ª. ed., p. 440; QUERALT JIMÉNEZ, J.J., *Derecho penal español, Parte especial, Delitos contra los intereses individuales y colectivos*, 3ª ed., Barcelona, 1996, p. 214; LANDECHO VELASCO, C.M./MOLINA BLÁZQUEZ, C., *Derecho penal español...*, op. cit., p. 254; SERRANO GÓMEZ, A., *Derecho penal*, op. cit., p. 434; MARCHENA GÓMEZ, M., en SERRANO BUTRAGUEÑO, I., Coord., *Código penal de 1995 (Comentarios y jurisprudencia)*, Granada, 1998, p. 1371; MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), *Curso de...*, op. cit., p. 288; ROBLEDO VILLAR, A., *Delitos contra el patrimonio...*, op. cit. p. 382.

¹⁵¹² Así, vid. CARBONELL MATEU, J.C., en AA VV, *Derecho penal, Parte especial*, op. cit., p. 473 y CARRASCO ANDRINO, M.M., en *La protección penal...*, op. cit., pp. 263 y ss.

(art. 279.2 CP) comparte con el tipo básico (art. 279.1 CP) el sujeto activo¹⁵¹³ y el objeto material, resultando la propia acción lo que los distingue¹⁵¹⁴.

En coherencia con lo anterior, el castigo de la utilización ilícita del secreto se ceñirá a dos sectores o grupos de casos. En primer lugar, a los supuestos en que, habiéndose accedido lícitamente a la información respecto de la que existe obligación de guardar reserva, el sujeto la emplea posteriormente en provecho propio (art. 279.2 CP) y, en segundo término, a aquellos en que, en virtud de una revelación ilícita (ya sea ex art. 278.2 o ex art. 279 .1 CP), el destinatario de la misma no se limita a recibirla sino que, además, la emplea en provecho propio (art. 280 CP). Sin embargo, no será punible la utilización o uso del secreto por parte de quien lo ha obtenido ilícitamente. De esta forma, se genera, en ese caso, una intolerable laguna legal, puesto que el aprovechamiento del secreto añade un plus de desvalor a la conducta de acceso ilícito o abusivo, que quedará sin reproche.

También desde una perspectiva penológica, diversas son las incoherencias que emergen. En primer lugar, resulta difícil identificar la *ratio* de la dulcificación –aunque ciertamente no excesiva– de la pena, que, en la utilización del secreto, sufre una rebaja respecto de la del tipo básico –de dos a cuatro años–, al ser aplicada en su mitad inferior. Ello ha conducido a

¹⁵¹³ Ello determina la conversión del art. 279.2 CP en un tipo especial propio. Esta configuración genera problemas en lo relativo a la participación delictiva, por ejemplo, en los supuestos en los que quien lleva a cabo el uso no es un obligado a mantener el secreto. Vid., al respecto, la disparidad de soluciones que ofrecen MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho penal económico, Parte especial, op. cit.*, pp. 86-87 y QUERALT JIMÉNEZ, J.J., *Derecho penal español, Parte especial, op. cit.*, p. 215.

¹⁵¹⁴ Sin embargo, esta relación (revelación, como tipo básico y uso, como modalidad atenuada) resulta, desde la perspectiva de la lógica jurídica, difícilmente asumible. Como se indicó al principio del análisis de esta modalidad típica, si algo resulta claro es que toda revelación del secreto puede integrar una forma de uso del mismo, pero no a la inversa. De esta significación de los términos, podría, a lo sumo, deducirse que la acción de usar integra el tipo básico, por ser más genérica, y la de revelar, la modalidad agravada, por devenir una forma específicamente insidiosa de uso del secreto.

que se cuestione el propio fundamento del privilegio¹⁵¹⁵. Sin embargo, un autorizado sector doctrinal estima razonable dicha atenuación y asienta su fundamento en diversas razones. Así, se esgrime que, con la utilización, se recorta menos la capacidad competitiva de la empresa en el mercado¹⁵¹⁶, existe un menor desvalor de resultado o una menor extensión de la lesividad de la conducta¹⁵¹⁷ o, simplemente, que el sujeto actúa a favor de sí mismo, en la medida que no se introduce en un conflicto ajeno¹⁵¹⁸. Asimismo, incluso se ha visto el fundamento de la atenuación, extramuros del desvalor de resultado, en el propio desvalor de acción, al entender que quien está en posesión de una información reservada de este tipo casi siempre habrá contribuido a la formación de la misma, por lo que se le acaba beneficiando¹⁵¹⁹.

A nuestro parecer, por el contrario, se trata de modalidades de ataque al bien jurídico de diverso contenido pero **de análoga gravedad**, hasta el punto que, según se ha advertido, establecer **a priori** una gradación lesiva entre ellas resulta imposible. Por ello, parece difícil afirmar, con carácter general, que la utilización recorta menos la capacidad competitiva de la empresa o que asume siempre menor potencialidad lesiva, ya que dicha

¹⁵¹⁵ Así es cuestionado por algunos autores partidarios de esta interpretación como modalidad atenuada; vid., en este sentido, MUÑOZ CONDE, F., **Derecho penal, Parte Especial**, 11ª. ed., p. 440; PRATS CANUT, J.M., "Descubrimiento y revelación de secretos...", en **Delitos relativos a la propiedad...**, *op. cit.*, p. 200; QUERALT JIMÉNEZ, J.J., **Derecho penal español, Parte especial**, *op. cit.*, p. 214; LANDECHO VELASCO, C.M./MOLINA BLÁZQUEZ, C., **Derecho penal español...**, *op. cit.*, p. 254; SERRANO GÓMEZ, A., **Derecho penal**, *op. cit.*, p. 434.

¹⁵¹⁶ TERRADILLOS BASOCO, J., **Derecho penal...**, *op. cit.*, p. 173.

¹⁵¹⁷ MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte especial**, *op. cit.*, p. 85.

¹⁵¹⁸ PÉREZ DEL VALLE, C., "La revelación de secretos de empresa...", en **Delitos relativos a...**, *op.cit.*, p. 124.

¹⁵¹⁹ GONZÁLEZ RUS, J.J., en AA VV (COBO DEL ROSAL, M., Dir.), **Curso de derecho penal**, *op. cit.*, p. 802.

peligrosidad dependerá del concreto ***modus operandi*** con que se acometa o ejecute la conducta, tanto si se trata de una revelación del secreto como de una utilización del mismo. Más extraña se muestra en el contexto en el que se integra la protección de los secretos empresariales la justificación relativa a que ***el sujeto no se introduce en un conflicto ajeno***, puesto que, a tenor de cómo se ha caracterizado el bien jurídico protegido en estos delitos, no parece que ése sea un extremo postulable. No se trata de si el sujeto interfiere en una relación o posición jurídica que ostenta el titular del secreto respecto a los demás competidores, sino de que al utilizar una información secreta que no ha sido fruto de su propio esfuerzo o actividad, lleva a cabo, al igual que si la revela, una conducta peligrosa para el interés del empresario, ***que entraña el riesgo de que el secreto pierda su valor*** y también un comportamiento ***que lesiona el interés general en la innovación***, esto es, el interés en el aseguramiento de que el esfuerzo innovador no será frustrado por ciertas actuaciones que permiten a otro aprovechar el secreto.

Por otra parte, retomando el análisis de las incoherencias que desde la perspectiva de la penalidad emergen, se observa que esa estratificación penológica establecida en el art. 279 CP, que penaliza la conducta de revelación y dulcifica la de utilización, es ignorada en el supuesto de que quien lleve a cabo estas conductas no sea el sujeto que ha accedido lícitamente, sino el tercero a quien se le han revelado los secretos (art. 280 CP). En este caso, tanto si el sujeto vuelve a revelar (revelación en cadena) como si decide utilizar el secreto en provecho propio, merece la misma pena.

Las consideraciones formuladas condicionan, en nuestra opinión, la toma de postura a favor de una interpretación de esta modalidad como tipo autónomo, al resultar una opción en la que concurren suficientes motivos que explican, ***de lege lata***, su mayor bondad y conveniencia político-criminal.

II) La utilización del secreto, como tipo autónomo.

El entendimiento de esta acción como una modalidad típica autónoma permite su aplicación sin necesidad de hacer referencia al tipo previsto en el art. 279.1 CP. Así, la acción de utilización resulta prevista específica y separadamente, como modalidad diversa al acceso y a la revelación.

De este modo, la utilización, como forma específica de explotación del secreto, resultará aplicable tanto en los supuestos en que el acceso es ilícito, como en aquellos en que el sujeto activo está legitimado para acceder al secreto. Así, en el primer caso, se aplicará un concurso medial de delitos (arts. 278.1 y 279.2 CP), puesto que concurre una pluralidad de hechos que da lugar a varios delitos (el acceso y la utilización) unidos en relación de medio a fin¹⁵²⁰ y, en el segundo, será de aplicación únicamente el art. 279.2 CP, que, **de facto**, quedará reservado para los supuestos de uso con acceso lícito¹⁵²¹.

¹⁵²⁰ En la utilización de un secreto al que se ha accedido ilícitamente, lo habitual será que esta pluralidad de hechos y de delitos se encuentre vinculada en relación de medio a fin. Aunque parece difícil imaginar, en este caso, que se dé un concurso real de delitos (en esta categoría se entienden excluidos los casos de concurso medial; así, vid. MIR PUIG, S., **Derecho penal, Parte general, op. cit.**, p. 665), si fuera el caso, ésa sería la calificación.

¹⁵²¹ Ello permite llegar a una conclusión distinta de la sostenida por MARTÍNEZ-BUJÁN PÉREZ, C., **Derecho penal económico, Parte especial, op. cit.**, p. 87, para el supuesto en que el sujeto obligado a guardar reserva utilice el secreto en provecho propio (creando su propia empresa del ramo de que se trate) y además divulgue el secreto a otras personas para que éstas se aprovechen del mismo (creando sus propias empresas). Según el citado autor, en este caso, no puede haber un concurso real –homogéneo– de delitos, sino un solo delito del tipo básico que consume el desvalor de la conducta constitutiva del tipo atenuado. En sentido análogo, vid. PÉREZ DEL VALLE, C., “La revelación de secretos de empresa...”, en **Delitos relativos a...**, *op.cit.*, p. 141. Sin embargo, a nuestro parecer, **a priori**, la solución debería ser la que, a continuación, se indicará, tanto si se caracteriza el uso como un delito autónomo como si se concibe como una modalidad atenuada. En ambos supuestos, al tratarse de varios hechos distintos y, por tanto, de varias infracciones (utilización y revelación) y no configurarse ninguna de ellas medio necesario para cometer la otra, suscitaría un **concurso real de delitos**. Así pues, mientras que los autores mencionados parecen resolver estas situaciones conforme a las normas del concurso de leyes, en mi opinión, dichas hipótesis deberían reconducirse al concurso de delitos.

Asimismo, esta interpretación permite establecer una graduación de la pena adecuada a los diversos *modi operandi* en que puedan acometerse este tipo de comportamientos. En el caso de que se produzca una utilización del secreto al que se ha accedido ilícitamente, nada impide apreciar un concurso medial de delitos (arts. 278.1 y 279.2 CP), que determinará la posibilidad de imponer la pena prevista para la infracción más grave, en su mitad superior, esto es, la pena de prisión de tres a cuatro años¹⁵²²; si se produce una utilización del secreto, al que se ha accedido legítimamente, la pena será de dos a tres años; y, por último, si se usa el secreto que se ha obtenido fruto de una revelación ilícita, la pena establecida en el art. 280 CP es la de prisión de uno a tres años.

De este modo, no sólo se logra evitar una indeseable laguna punitiva (la utilización del secreto con acceso ilícito), sino que, desde el punto de vista de la penalidad, se refuerza el carácter autónomo pero de análoga e ingraduable –apriorísticamente-- gravedad de las modalidades atentatorias de revelación y de utilización.

Así, el marco punitivo de estas modalidades se integrará, en el caso de la revelación, por una pena de prisión de dos a cuatro años o –si hay acceso previo ilícito-- de tres a cinco y, en la utilización, de dos a tres o –con acceso previo ilícito-- de tres a cuatro. De este modo, surge una franja intermedia en la que se solapa un mínimo marco penal (prisión de dos a tres años) que permitirá al juzgador singularizar en cada caso la concreta gravedad y peligrosidad que la revelación o la utilización del secreto, dependiendo del *modus operandi*, puede comportar. Ello facilitará que, en un supuesto concreto, la revelación, por ejemplo, mediante rueda de prensa, merezca el mayor reproche y que, por el contrario, la ejecución de esa

¹⁵²² La pena prevista en el art. 278.1 CP es prisión de dos a cuatro años y la del art. 279.2 CP, de dos a tres años.

misma modalidad pero con otros medios menos lesivos, pueda llevar aparejada una pena menor que la utilización.

Esta interpretación, sin duda voluntarista, de la explotación del secreto como tipo autónomo no se encuentra, sin embargo, exenta de problemas.

En primer lugar, surgen inconvenientes de orden gramatical. Así, no hay una referencia clara al sujeto activo de la acción, lo que deviene especialmente conflictivo al configurarse como un delito especial propio la primera modalidad de acción. En segundo término, la fijación de la pena se arbitra a partir de la referencia de la modalidad del tipo básico de revelación del secreto. Estos escollos, en gran medida, traen causa de su regulación conjunta en un mismo precepto, puesto que –a nuestro parecer-- el resto de lagunas y disparidades se vinculan a dicha falta de independencia.

Sin embargo, no se trata de limitaciones insoslayables. Respecto a los sujetos, no hay una referencia expresa sino implícita. De ahí que, con arreglo a una interpretación teleológica, tendente a evitar lagunas y sin incurrir en una interpretación extensiva, resulte solventable la objeción relativa a que el sujeto activo de la acción deba ser el mismo que el de la modalidad anterior y, por tanto, un sujeto que conoce lícitamente y que se halla obligado a guardar reserva. En cuanto a la fijación de la pena, se trata de una defectuosa técnica de tipificación¹⁵²³.

¹⁵²³ Esto es, en el vigente código penal, el arbitrio de la fijación de la pena de modo independiente o a partir de la referencia de otra modalidad no parece asumir una significación unívoca. Así, en algunas modalidades típicas respecto de las que media una relación de tipo básico- tipo agravado, la penalidad se establece autónomamente y no por referencia al precepto sobre el que se construye (vid., por ejemplo, los delitos de homicidio y homicidio agravado o asesinato y cualquiera de las modalidades típicas previstas en los delitos contra la libertad e indemnidad sexuales, entre muchos otros).

Ahora bien, esta interpretación no impide reclamar la conveniencia de formular una propuesta **de lege ferenda** de mayor pulcritud y claridad, que subsane las insuficiencias indicadas. Así, se desvela fundamental prever la utilización del secreto como modalidad de ataque autónoma en un tipo independiente y asignarle, en consecuencia, una pena también autónoma y no por referencia a otro precepto.

Concluido el examen de las acciones típicas, conviene efectuar ya una sucinta recapitulación y conclusión crítica de las consideraciones formuladas.

VI. Recapitulación y propuesta de “lege ferenda”.

Las diversas modalidades atentatorias de los secretos se hallan, en su mayoría, expresamente previstas por el código penal en los preceptos reguladores de la materia objeto de estudio (así, por ejemplo, la acción de apoderamiento, la relativa al control audiovisual clandestino y control ilícito de señales de comunicación, la revelación, difusión o cesión y, por último, la utilización). Otras, sin embargo, se encuentran todavía ayunas de referencia legal en estos delitos (así, la reproducción, el “apoderamiento” abusivo y la destrucción, alteración o inutilización de los secretos).

Resulta incontrovertible que, con la incorporación **ex novo** de alguna de estas acciones y con la nueva redacción otorgada a otras de ellas ya previstas en el anterior código, se ha avanzado notablemente y se ha logrado acompasar el derecho penal a las características de modernidad, globalidad e informatización de la actual realidad económica y empresarial. Ahora bien, también es cierto que la protección de los secretos de empresa adolece de bondad sistemática y que el desacierto en el orden de las

acciones hace perder matices y perfiles, genera lagunas legales y evidencia dislates valorativos. Esta consideración crítica ha sido inferida de diversas cuestiones dudosas e insatisfactorias, que han sido señaladas en el análisis de estas modalidades típicas y a cuya breve recapitulación se procede.

l) Por lo que se refiere a la primera de las modalidades atentatorias, que se integra por el **acceso ilícito** a la información, se prevén expresamente dos conductas distintas, a saber, el apoderamiento y la interceptación.

El **apoderamiento** comprende conductas de captación intelectual, sin desplazamiento físico (apoderamiento de datos) y conductas de apoderamiento físico subrepticio de los objetos que incorporan el secreto (apoderamiento de documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo). Así pues, **de lege lata** esta modalidad permite abrazar todos aquellos objetos en los que puede quedar plasmada la información empresarial de carácter secreto.

La **interceptación o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción** abraza las conductas reconducibles a la idea de control auditivo (grabación, escucha o interceptación de comunicaciones habladas) o visual (filmación-captación de imágenes), así como los comportamientos de interceptación, grabación o reproducción ilícita de otros medios de comunicación, como las comunicaciones por telefax o a través de una red informática, ya sea de área local (**intranet**) o de área amplia (como, por ejemplo, Internet). Con su previsión, se ha afrontado, satisfactoriamente, el espionaje empresarial acometido por medios informáticos. En este caso, la deficiencia más importante se produce, por lo que se refiere a la conducta de interceptación en una intranet, en los supuestos de extralimitación, que, también resultan problemáticos en el ámbito del apoderamiento.

II) Pues bien, frente a las conductas analizadas (apoderamiento e interceptación), que, de modo expreso, aparecen recogidas en el código, no se prevén otras modalidades de ataque, que, estrechamente vinculadas a los abusos informáticos, pueden, de igual forma, incidir sobre el secreto de empresa, como, por ejemplo, la reproducción, el “apoderamiento” abusivo y la destrucción, alteración o inutilización del secreto.

a) La conducta de **reproducción** comprende, esencialmente, la copia de la información acometida por medios informáticos, a fin de procurarse certeramente el contenido del secreto, conformándose como una modalidad de ataque de entidad y desvalor distinto --en algunos casos, al menos-- a los de la conducta de acceso. El código, sin embargo, no contempla la conducta de reproducción como modalidad de ataque independiente. Únicamente aparece contemplada en la modalidad de interceptación, en cuya regulación el código sanciona dicha acción y cualquier reproducción posterior. Por el contrario, no aparece prevista en la modalidad de apoderamiento, pese a lo cual, en la medida en que la conducta de reproducción siempre implicará una conducta previa de acceso, podrá formar parte de su ámbito de tutela, aunque, sin duda, **el apoderamiento puede constituir un medio comisivo menos grave** que la reproducción.

b) El “**apoderamiento**” **abusivo** se integra por el acometido con autorización para acceder a los datos o adueñarse de los soportes, pero abusando de dicha autorización --o sea, no en la forma en que debiera hacerlo, sino dándole un uso distinto--. Esta modalidad atentatoria reconducible al abuso de funciones o a la extralimitación, no se halla prevista ni en el ámbito del apoderamiento ni en el de la interceptación.

c) Los comportamientos de **destrucción**, **alteración** o **inutilización**, como modalidades de ataque sobre el secreto de empresa, tampoco se

hallan expresamente previstos en la regulación de estos delitos. Así, para subsanar esta laguna debe acudir a la aplicación de otros preceptos y, en concreto, al tipo regulador del sabotaje informático, contemplado en el art. 264.2 CP. Sin embargo, la propia ubicación sistemática de los daños informáticos en los delitos contra el patrimonio y la compleja identificación del bien jurídico protegido entorpecen su idoneidad para reprimir estas modalidades de ataque sobre el objeto material de los delitos reguladores del secreto de empresa y acaban procurando al bien jurídico protegido por estos últimos una tutela asistemática.

III) La **revelación, difusión o cesión** del secreto, constituye otra de las modalidades de acción típica, que se halla expresamente contemplada en los delitos relativos a la protección del secreto empresarial, tanto si el sujeto ha accedido ilícitamente a la información o legítimamente, pero con deber de guardar reserva. En la interpretación de estos tres términos no se han podido encontrar criterios unívocos que deslinden con claridad sus respectivos ámbitos de aplicación, de modo que asumen una significación análoga o equivalente, que permite cubrir **de lege data** cualquier posible laguna pero que entorpece la exégesis de estas modalidades, al forzar una inteligencia distinta para cada uno de ellos.

IV) La **utilización** del secreto, que constituye la última de las modalidades atentatorias, supone el aprovechamiento económico del secreto, lo que determina el rechazo de una interpretación amplia del término, como concepto o modalidad omnicomprendiva de la anterior acción. Esta modalidad se halla expresamente recogida en el art. 279.2 CP. La técnica empleada en su configuración (regulación en un único precepto con la modalidad de revelación, difusión y cesión; ausencia de remisión a los sujetos y, especialmente, determinación de la pena a partir de la del tipo de la revelación) han suscitado dispares pronunciamientos doctrinales sobre su

condición de **modalidad atentatoria privilegiada** y, por tanto, dependiente de la conducta básica de revelación del secreto por quien ha accedido a él legítimamente, pero con deber de guardar reserva o su calificación como **tipo autónomo**. A nuestro parecer, esta última opción se ha estimado preferible, ya que su entendimiento como acción típica autónoma autoriza su aplicación sin necesidad de hacer referencia al tipo previsto en el art. 279.1 CP y, por tanto, como modalidad diversa al acceso y a la revelación. Ello, a su vez, permite salvar indeseables lagunas legales (como la utilización del secreto por quien accede a él ilícitamente) y explicar una más adecuada gradación en la penalidad.

Así pues, esta delimitación del ámbito de lo punible desde el examen de las modalidades típicas ha desvelado, **de lege lata**, algunos vacíos legales y ciertas consecuencias disfuncionales. Esta conclusión crítica alcanzada reclama, pues, en buena lógica, esbozar una sucinta propuesta **de lege ferenda**.

El modelo de sistemática postulable más adecuado, desde el punto de vista de las acciones típicas, no implica modificar la naturaleza que, en el código, asumen estos delitos (apoderamiento, interceptación, difusión, revelación, cesión y utilización) y descansa en la incriminación de las cuatro modalidades atentatorias analizadas, a saber, el acceso, la destrucción, alteración e inutilización, la comunicación y la explotación. Las consideraciones que, a continuación, se formulan a propósito de cada una de estas acciones, asumen validez a modo de pauta o hipótesis de trabajo sobre la que deberá reflexionarse con mayor detenimiento.

l) La modalidad de **acceso** al secreto, que comprendería el apoderamiento y la interceptación, en cuanto ambas representan diversas formas de acceso, debería descansar conceptualmente sobre la ilicitud de la conducta dimanante de no ser fruto del propio esfuerzo. Este entendimiento debe llevar a aprehender las diversas modalidades de ataque que pueden poner en peligro el bien jurídico e incidir sobre el objeto material, caracterizado en este caso por su especial complejidad y su almacenaje en soporte informático.

Así, la modalidad de ataque relativa a la reproducción debería asumir relevancia y autonomía penal, tanto si la lleva a cabo un sujeto no autorizado para acceder al secreto --en cuyo caso la reproducción puede ser un plus--, como en los casos en que no hay tal acceso ilícito, ya que no hay previo apoderamiento o se copia porque se está autorizado. En esta medida, el legislador debería hallar una fórmula que permitiese captar la diferente gravedad que puede suponer la conducta de acceso y la de reproducción, como modo de aseguramiento del secreto.

Análogamente, debería ser también una conducta subsumible en la modalidad que recoja estos atentados al secreto, el “apoderamiento” abusivo, esto es, el apoderamiento que acomete alguien con autorización para acceder a los datos, pero no en la forma en que debiera hacerlo, sino dándole un uso distinto. Todo ello quizá podría lograrse, de una parte, asentando el precepto sobre **la adquisición o el aseguramiento de la información de forma indebida**, sin autorización o con ella, pero extralimitándose y, de otra, ampliando el elemento subjetivo del injusto al ánimo de obtener provecho, propio o de tercero, o de perjudicar al poseedor del secreto.

De igual modo, la **concreta forma de obtención de los datos debería asumir relevancia**, debiéndose contemplar las distintas modalidades de ataque al objeto y también trasladar la divergencia del desvalor de las mismas al ámbito de las consecuencias jurídicas. En este sentido, quizá convendría reflexionar acerca de la conveniencia de distinguir las conductas de **apoderamiento subrepticio de soportes** u objetos que se refieran al secreto y de captación intelectual del mismo --que no sea fruto de un abuso informático-- y las **conductas de acceso ilícito** a la información, mediante la utilización de las nuevas tecnologías de la información.

II) Una vez incriminado el acceso a la información, sería aconsejable la creación de una modalidad específica, dirigida a sancionar las conductas de alteración, destrucción o inutilización de la información que conforma el objeto del secreto de empresa. Esto es, un tipo inserto en los preceptos reguladores de la violación de secretos y destinado a proteger el bien jurídico, en este caso, el interés del empresario en mantener la reserva de ciertas informaciones, que habitualmente se almacenan en equipos informáticos y se transmiten por circuitos telemáticos, para lo cual es intrínsecamente indispensable, preservar la integridad y disponibilidad de esa información que, digitalizada, deviene especialmente vulnerable y sensible. Así pues, en la formulación legislativa de esta modalidad de ataque deberá tenerse en cuenta la configuración del objeto material del delito y del propio bien jurídico y arbitrar en atención a estas peculiaridades una tutela adecuada, con independencia de la concreta técnica legislativa por la que se opte.

III) A continuación debe preverse la revelación del secreto, en cuya tipificación sería deseable el empleo de un único verbo capaz de aprehender el núcleo del injusto, que descansa en la conducta de comunicación del secreto a un tercero no autorizado. La posible incorporación de diversas

modalidades de acción, en función de si se trata de una revelación minoritaria a una o varias personas concretas y determinadas o, por el contrario, de una divulgación generalizada, sólo cobra sentido si posteriormente desea trasladarse el diverso desvalor de estas conductas –a nuestro juicio, cuestionable-- a una penalidad estratificada en atención a la diversa gravedad. Sin embargo, dada la especial sensibilidad y expugnabilidad del secreto de empresa, cuya revelación a una única persona supone la pérdida de control del mismo y, en esa medida, la puesta en peligro del bien jurídico protegido, se estima preferible la incriminación de la comunicación de la información, independientemente del número de destinatarios, puesto que no parece desvelarse como un criterio certeramente indicativo de menor o mayor peligrosidad para el bien jurídico.

Sin duda, en la línea adoptada por el vigente código, esta conducta deberá proyectarse tanto sobre la revelación de un secreto al que se ha accedido o asegurado ilícitamente como sobre la del secreto al que se ha accedido legítimamente, con la correspondiente estratificación penológica. Asimismo, en virtud de la caracterización de estas acciones como delitos de participación necesaria, el tipo que se destine a sancionar la comunicación del secreto, deberá comprender asimismo las conductas de «revelación en cadena», esto es, la comunicación del secreto por quien lo haya conocido en virtud de esa comunicación típica que castiga de modo principal el precepto. Así, la conducta de comunicación ilícita del secreto abrazaría la revelación de secretos a los que se ha accedido ilícitamente, lícitamente o fruto de una revelación ilícita previa (revelación en cadena).

IV) La última conducta o modalidad de acción típica debe ser la explotación del secreto, con el ánimo de obtener provecho, propio o de tercero, o de perjudicar al poseedor del secreto, como conducta de significación e importancia autónoma, al igual que las tres anteriores. Así,

esta conducta comprenderá, la explotación del secreto, con independencia de que se haya accedido a él abusiva o legítimamente. Asimismo, también quedará incluida en el precepto regulador de esta modalidad de ataque, la explotación llevada a cabo por quien accedió al secreto como destinatario o receptor de una comunicación ilícita --reverso de la anterior modalidad de comunicación--.

En cuanto al marco punitivo de estas acciones, existen varias opciones legislativas. Así, una de ellas radica en el establecimiento de una penalidad escalonada. De este modo, en el primero de los casos --explotación de un secreto al que se ha accedido ilícitamente--, la pena deberá verse incrementada; en el segundo supuesto --explotación de un secreto cuyo acceso ha sido lícito--, será de menor gravedad y en el último --explotación de un secreto que se conoce fruto de una revelación ilícita--, quizá la pena debería ser de análoga entidad al segundo de los supuestos o ligeramente superior.

La otra opción posible se cifra en establecer una pena única y autónoma para la explotación. De este modo, para los supuestos de explotación de un secreto cuya obtención ha sido ilícita, se debería acudir a las reglas generales del concurso, que, según se expuso, en este caso, daría lugar a un concurso medial de delitos.

CONCLUSIONES

I

El desarrollo tecnológico de la sociedad postindustrial del siglo XX ha generado un modelo social, cuyo progreso depende, en gran medida, de los sistemas de información y comunicación y en el que la información, lógicamente, se configura como un bien de inusitado valor. Este incremento del valor de la información en la sociedad actual y, específicamente, en la economía de mercado, también asume una especial incidencia en el seno de la empresa. De una parte, la información empresarial reservada se erige en un instrumento de primer orden, imprescindible para subsistir y progresar en un mercado internacional intensamente competitivo. De otra, la integración en Internet de las actividades empresariales y el proceso de globalización que caracteriza la economía moderna suscitan profundas transformaciones y posibilitan una nueva forma de investigación y una nueva forma de organización de la producción y de la comercialización, caracterizada por su dimensión transnacional. Así, en este mercado, definido por el carácter mundial de su estructura, estrategia y funcionamiento, el secreto empresarial se erige en una importante arma competitiva de los agentes u operadores económicos profesionales, que serán juzgados, ante todo, por su eficiencia. En esta medida, una correcta comprensión jurídica del secreto empresarial, así como el arbitrio de su régimen jurídico se revelan como una cuestión crucial para el intercambio y el crecimiento económico.

II

La característica común del derecho español y de los ordenamientos de otros países del ámbito europeo se cifra en el amplio abanico de expresiones a las que el legislador recurre para hacer referencia al secreto empresarial, careciéndose, pues, de una terminología unitaria. A ello debe

añadirse que, pese a su trascendencia económica y su frecuente aparición en textos normativos, el secreto empresarial no ha sido objeto de definición en derecho español, ni tampoco en los países de la Unión Europea. La multivocidad empleada por el legislador para aludir a los secretos atinentes a la actividad empresarial y un apenas formulado concepto de los mismos, ha suscitado incertidumbre en la utilización de las especies que lo integran (secreto industrial y secreto comercial), de una parte y necesidad de recurrir a un concepto omnicomprensivo capaz de cubrir las constantes lagunas legales, de otra.

III

La dispersión terminológica y la ausencia de definición legal en derecho español, explica, también, la opción metodológica asumida en este trabajo, que reclama examinar, en primer lugar, los requisitos que configuran jurídicamente el secreto y formular, con posterioridad, su concepto a efectos penales. En esta progresión secuencial de construcción jurídico-penal del secreto, se ha corroborado la bondad de la denominación «secreto de empresa» para designar el objeto de estudio y, asimismo, el desacierto de su equiparación con cualquiera de las especies que lo integran (secreto industrial, secreto comercial). Así pues, se parte de esta noción amplia designada por la expresión «secreto de empresa», como fórmula idónea que engloba la totalidad de la información que integrará su objeto.

IV

Para acometer esta verificación es necesario previamente saber qué presupuestos o requisitos estructuran internamente el concepto de secreto. Una información constituye secreto empresarial cuando en ella concurren los

siguientes requisitos: carácter reservado, valor competitivo y voluntad de mantenerla en secreto por parte de su titular.

V

El requisito esencial y básico radica en que la información posea el carácter de reservada u oculta, en cuya consecución deviene imprescindible la falta de divulgación pero no una reserva absoluta. Así, acerca del grado relativo de reserva exigible para que un conocimiento permanezca oculto, puede decirse que una información se mantiene secreta mientras no es generalmente conocida ni fácilmente accesible. En cuanto al momento en que se produce la divulgación, una información es secreta cuando los terceros y, en particular, los terceros interesados en disponer de ella, no tienen conocimiento en general de la misma, bien de la totalidad, bien de una parte esencial o bien del resultado de la interacción de sus partes. Por lo que atañe a la notoriedad, ésta se produce cuando una información es fácilmente accesible para cualquiera que esté interesado en conocerla (generalmente, un competidor), sin que se requiera para su obtención y/o combinación, un particular esfuerzo cualitativo --experiencia, conocimientos-- o cuantitativo --de inversión, en tiempo o costes--.

VI

El segundo requisito se cifra en el interés económico que el secreto encierra para la empresa, puesto que la ventaja o mejora que comporta, en cualquiera de sus diversas parcelas, constituye una pieza de primer orden para el fortalecimiento de su capacidad competitiva y para el mantenimiento de su posición o de su situación en el mercado. La interpretación o ponderación de dicho interés económico se articula bajo criterios objetivos en función de la ventaja competitiva de la información, que no debe

afirmarse o negarse en términos absolutos o abstractos, esto es, en relación con el resto de empresarios competidores, sino en términos relativos o particulares, en atención a las estrategias y actuaciones que en particular permite realizar a su titular. El valor económico de la información se singulariza, pues, en virtud de las necesidades y preferencias de su poseedor, lo que determina que pueda diferir de un titular a otro. Así, el valor competitivo de la información es un valor relativo, referencial, que permite a su poseedor actuar estratégicamente y organizar su actividad económica del modo más rentable y beneficioso posible. En este sentido, la interpretación del contenido de este requisito lo aproxima más al concepto de «valor de uso» que al de «valor de mercado». En consecuencia, el perjuicio económico que el acceso y la revelación ilícita del secreto puede acarrear al empresario no es interpretado desde una perspectiva o entendimiento clásico del mismo, como lesión, menoscabo o daño patrimonial efectivo (daño emergente y lucro cesante) y, por tanto, económicamente cuantificable. Antes bien, en el contexto competitivo en el que se inserta el secreto, la producción del perjuicio se vincula con la pérdida del valor de la información y, por tanto, con la desaparición de la ventaja o de la mejora competitiva que provoca su revelación. Sólo en la medida en que este perjuicio se ve anudado, en último término, a la perturbación del derecho a realizar y a organizar una actividad económica en el mercado, puede ser calificado de económico.

VII

La voluntad de mantener el secreto constituye el último requisito imprescindible para la configuración jurídica del secreto empresarial. En su entendimiento deviene especialmente relevante que esta voluntad o elemento subjetivo sea reconocible externamente, esto es, que pueda ser percibida de forma clara, cercenando cualquier duda respecto al ánimo del

titular. Así, la manifestación de la voluntad puede llevarse a cabo expresamente --a través de una cláusula contractual o cualquier otra instrucción expresa-- o tácitamente --mediante la adopción de conductas o la ejecución de actos de los que se deduzca la voluntad del titular--.

VIII

De la aplicación de los requisitos configuradores analizados dimana el propio concepto penal de secreto de empresa. Conforme lo anteriormente expuesto, 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. Así pues, lejos de hallarnos en presencia de un figura unitaria, el secreto empresarial aglutina heterogéneas informaciones concernientes a los diversos ámbitos que componen la actividad empresarial, esto es, industrial, comercial u organizativo. Esta noción de secreto, condicionada por el bien jurídico protegido, entronca con la naturaleza intrínseca del secreto como específico y estratégico acto de iniciativa económica.

IX

Tras la caracterización jurídica fundamentadora del concepto de secreto de empresa, es asimismo imprescindible un adecuado entendimiento del secreto, como elemento o técnica jurídica instrumental, en sí mismo vacío de contenido, que puede estar al servicio y tener por objeto múltiples intereses (secreto de estado, secreto instructorio, secreto personal, secreto industrial, etc.), sin confundirlo con el objeto de protección a cuyo servicio se halla. En consecuencia, el secreto no constituye **per se** un interés, un valor o un bien jurídico autónomo, sino que se revela como una técnica enderezada a la

protección de bienes jurídicos relevantes de muy diversa naturaleza (distintos intereses estatales, el derecho a la intimidad, intereses de impronta económica o patrimonial, entre otros) y que, por tanto no debe ser equiparada al objeto jurídico de protección.

X

Consecuencia de lo anterior es que una de las notas definitorias que reúne la información que puede ser objeto de secreto de empresa es la de ser un bien esencialmente económico, condición que deriva de su carácter intangible, no apto para su inmediato disfrute económico, con valor patrimonial y susceptible de ser repetido indefinidamente en su forma corpórea. En esta medida, la nota que verdaderamente sintetiza la esencia del secreto empresarial y, por ello, lo caracteriza, radica en su cualidad de bien económico con contenido y valor patrimonial.

XI

Configurado como bien o interés esencialmente económico, la especificidad funcional propia del secreto, que lo diferencia del resto de valores o intereses económicos susceptibles de tutela penal (de las modalidades de propiedad industrial e intelectual y, en suma, de otros delitos contra el patrimonio o el orden socioeconómico), viene suministrada por el derecho de la competencia y, en concreto, por la competencia desleal. En esta medida, el acercamiento desde la perspectiva económica y jurídico-mercantil de estas instituciones ha sido indispensable a los efectos de delimitar y precisar el bien jurídico protegido en los artículos 278 a 280 del Código penal. Ello reclama la necesaria vinculación entre el secreto y las reglas de la competencia, en general y la ley de competencia desleal

española, en particular, como presupuesto indispensable para la interpretación de los preceptos del código penal.

XII

El derecho contra la competencia desleal se configura como ordenamiento general de la actividad concurrencial de todos los agentes económicos (generalmente profesionales) en el mercado mediante normas objetivas de conducta, abandonando las fronteras del derecho privado clásico para ingresar en el ámbito del derecho económico de intervención. Se trata, así, de un derecho ordenador de las relaciones en el mercado, reconociendo y protegiendo, junto a los intereses de los competidores, los de los consumidores y el interés público en el mantenimiento de un orden concurrencial no falseado. La finalidad perseguida por la disciplina se cifra en la competencia económica como principio político, que integra en su defensa los intereses de todos aquellos cuya actividad y necesidades económicas y sociales se desenvuelven y satisfacen en el mercado, incluido el interés público.

XIII

Fruto de la recepción generalizada del modelo social de competencia, la vigente ley de competencia desleal española consagra, asimismo, una tutela de la competencia, entendida no sólo como manifestación de un derecho individual del empresario a la libre iniciativa económica, sino, en una indubitada dimensión social, como normativa o principio regulador político-institucional de organización y de ordenación de las relaciones económicas en el mercado. Así pues, la competencia económica cuya tutela interesa el ordenamiento español se asienta en un heterogéneo fundamento, de carácter individual de una parte y de marcada impronta instrumental o

funcional de otra. El legislador español ha abandonado el recurso a la disciplina de la competencia desleal como mecanismo de solución de conflictos entre empresarios competidores y la consagra como instrumento de control de los comportamientos ejercidos por los agentes económicos en el mercado y, por tanto, como derecho ordenador y organizador de las relaciones económicas que en el mismo se suscitan. La construcción del ilícito de deslealtad concurrencial ya no se articula sobre la lesión de derechos subjetivos del empresario competidor, sino en torno a la infracción de normas objetivas generales de conducta que afectan por igual a todos los que acceden al mercado para intervenir económicamente y que fijan los lindes institucionales a su libre actuación en el mercado.

XIV

El criterio delimitador del ilícito desleal se define por la contrariedad objetiva de la conducta a las exigencias de la buena fe. Este criterio de la buena fe consagra la naturaleza del ilícito desleal como abuso institucional de la competencia y se alimenta del principio de competencia por los méritos, por el propio esfuerzo o por eficiencia de las prestaciones. De esta manera, la competencia económica es considerada por el ordenamiento como un bien en sí mismo, que, si se basa en el propio esfuerzo y en la mejora de las propias prestaciones, estimula a los sujetos económicos, organiza y ordena sus relaciones y logra la óptima asignación de recursos. En suma, pues, la delimitación entre lo lícito e ilícito en materia de competencia desleal descansa en el principio de competencia por el propio esfuerzo, en cuya virtud los concurrentes deben acudir al mercado de forma independiente y armados sólo de su propia eficiencia. La proyección de estas conclusiones asume una singular importancia en la protección del secreto.

XV

El empresario debe presentarse en el mercado y competir en base a la calidad de sus propias prestaciones. De modo que, cuando en la lucha económica los empresarios compiten no en base a su propia actividad, sino empleando medios o modos reprobables al objeto de esquivar el riesgo intrínseco a la diaria pugna competitiva, se altera inadmisiblemente la igualdad de las reglas del juego. En estos casos, la competencia ya no puede encontrar justificación en su propia capacidad de funcionamiento o rendimiento (Leistungsprinzip), que reclama la correspondencia entre el esfuerzo realizado por el competidor y el resultado obtenido. Por ello, cualquier perjuicio producido como consecuencia de una actuación falseadora de la competencia resulta ilícito. De ahí que la violación de secretos se configure como un acto de competencia desleal, reputándose el daño que se ocasiona intolerable e injusto puesto que el aprovechamiento indebido del esfuerzo ajeno no forma parte de una lucha concurrencial libre y eficaz.

XVI

La tutela del secreto empresarial pretende preservar los resultados fruto del propio esfuerzo y fomentar, así, el avance y el progreso también mediante el propio esfuerzo y sin apropiación indebida del esfuerzo ajeno. El bien jurídico protegido se cifra, precisamente, en el interés económico del empresario en el mantenimiento de la reserva. Este interés reviste dos notas esenciales que deben ser subrayadas.

XVII

Se trata de un interés de contenido económico que, por tanto, no debe ser confundido con el simple interés o voluntad del empresario en el

mantenimiento del secreto de cualquier información. La restricción que debe operar para seleccionar las informaciones que pueden ser relevantes para el derecho y constituir secreto empresarial ha sido ya ejercida en la propia configuración jurídica, utilizada como criterio delimitador del concepto penal.

XVIII

El interés económico tutelado como bien jurídico es un interés subjetivo del empresario en mantener la reserva sobre los frutos de su propia actividad. La objetivación necesaria para que devenga relevante jurídicamente sin incurrir en arbitrariedades y excesos se ha producido en su vertebración jurídica, a través de un doble diafragma. En primer término, la propia configuración jurídica del secreto se asienta sobre la corroboración de requisitos de carácter general proyectables a cualquier información o conocimiento; en segundo término, el valor económico o competitivo que debe ostentar la información asume carácter objetivo-subjetivo. Esto es, la exigencia de este valor económico objetivo-subjetivo permite despreciar la información de escasa entidad (primera subsecuencia enjuiciadora de tenor objetivo), que no permita proseguir en la averiguación del valor competitivo que asume para ese empresario en concreto (segunda subsecuencia valorativa de tenor subjetivo o relativo).

XIX

Con la tutela del secreto se persigue, además de la tutela de ese interés económico o patrimonial, preservar que el propio esfuerzo innovador, el avance o el éxito empresarial no se verán frustrados por conductas desleales, que, al no basarse en la propia eficiencia, no pueden ser toleradas por el mercado. Según se ha expuesto, la competencia cumple funciones político-económicas y, entre ellas, la función de selección, en cuya

virtud recompensa con el máximo beneficio a los empresarios que ofrecen las mejores prestaciones en el mercado y elimina de este último a los operadores ineficaces. Así, no son argumentos de moral empresarial los que explican la deslealtad de estas conductas sino de eficiencia económica. El mercado sólo puede soportar la adquisición, la divulgación, la revelación de secretos, la destrucción de vínculos contractuales ajenos, entre otras conductas, si ello responde a una mayor eficiencia de las prestaciones propias. En esta medida, con la protección jurídica del secreto se persigue también, aunque sea mediatamente, preservar y fomentar el avance y el progreso mediante el propio esfuerzo y, en suma, la competencia por las propias prestaciones. El bien jurídico técnicamente protegido o primordialmente protegido asume, pues, un contenido claramente económico o patrimonial, pero su protección adquiere sentido y se acomete desde el derecho de la competencia desleal, de marcada impronta institucional y social.

XX

El secreto empresarial como bien esencialmente económico, cuya protección jurídica descansa en la preservación de los resultados del propio esfuerzo en la libre iniciativa empresarial y en el consiguiente fomento del avance industrial y comercial también mediante el propio esfuerzo y no a través de la apropiación del esfuerzo ajeno, a fin de conseguir el objetivo de un mercado competitivo, a saber, el triunfo de los mejores. A ello se endereza la especial tutela de la que son objeto los secretos empresariales por parte del ordenamiento y que no radica en el reconocimiento expreso de un derecho de exclusión ***erga omnes***, ni siquiera en el de un específico derecho subjetivo sobre el secreto en sí, ***sino que se configura como una facultad jurídica integrada en el más amplio derecho subjetivo a ejercer una actividad económica, reconocido en el artículo 38 CE***, cuyo contenido esencial se cifra

en la competencia económica. Así, el sistema o modelo económico constitucional, asentado en los artículos 1, 9.2 y 38 CE, determina una competencia convertida en principio normativo de ordenación de los procesos económicos, al que se anuda el respeto de la libertad material de los individuos y, en concreto, de la de los agentes económicos (incluido el consumidor).

XXI

El mantenimiento de los delitos reguladores del secreto de empresa (arts. 278 a 280 CP), que comparten casi identidad de hechos, con algunos ilícitos civiles (art. 13 LCD), resulta necesario y conveniente. En esta medida, dado que se trata de delitos perseguibles a instancia de parte (art. 287.1 CP), excepto cuando afecten al interés general o a una pluralidad de personas (art. 287.2 CP), acarrea diversas consecuencias, entre las que destaca la introducción en nuestro sistema procesal del principio de oportunidad. Esta posibilidad se revela un acierto que justifica la propia previsión de delitos en el código penal que también son ilícitos mercantiles y da cabida así al principio de intervención mínima en la fase de aplicación y ejecución de la ley penal.

XXII

El impacto que toda revolución tecnológica suscita ha afectado, de modo especialmente intenso, al ámbito socioeconómico y, en especial, al de la empresa. El concepto del secreto de empresa asume, pues, un inequívoco contenido de **carácter dinámico**. Este entendimiento resulta, por otra parte, completamente postulable si se tiene en cuenta la configuración del secreto como **bien esencialmente económico vinculado a la competencia e inserto de lleno en el mercado**. Ahondando en esta visión dinámica de la

información, se advierte que, en puridad, estos circuitos por los que transita serán, habitualmente, telemáticos, lo que suscitará peligros y modalidades de ataque especialmente insidiosas para el objeto de tutela. Así, la advertencia de estos peligros que se ciernen sobre el objeto jurídico lleva a reflexionar sobre las nuevas necesidades de tutela y, en concreto, sobre las facultades que deben integrarlo. En suma, si la necesidad de una **protección jurídica eficaz** de los intereses referidos resulta indiscutible, desde luego, la eficaz salvaguarda de los bienes jurídicos, mediante la adecuada selección de las técnicas de tutela, exige atender a los **condicionamientos de orden fáctico y valorativo**, esto es, a los presupuestos indispensables para una prognosis racional de eficacia, lo que deberá proyectarse especialmente en la determinación de los objetos y de las técnicas de tutela idóneas.

XXIII

En cuanto al primer aspecto, el bien jurídico no puede reducirse en su significado a meras facultades de exclusión de terceros, sino que debe aglutinar facultades de control y de gestión sobre los datos que se mueven en los circuitos telemáticos.

XIV

En cuanto a las técnicas de tutela, se precisan las técnicas adecuadas que permitan captar la perspectiva material de injusto que integra el delito, que no será posible radicar en el daño producido y, en ocasiones, ni tan siquiera en la puesta en peligro concreto del bien jurídico. Frente a los peligros suscitados en este ámbito, el empleo de tipos delictivos de peligro abstracto puede ser una técnica idónea, siempre que se cumplan dos requisitos esenciales. En primer lugar, que la conducta prohibida por el legislador

venga especificada con precisión; en segundo término, que la prohibición se refiera directamente a bienes jurídicos claramente determinados.

XXV

La caracterización jurídica del secreto de empresa y la aproximación a los intereses protegidos con su tutela desde el derecho de la competencia económica y, en concreto, desde el derecho de la competencia desleal se ha llevado a cabo como sedimento indispensable en la elaboración de una teoría general sobre el bien jurídico en estos delitos. El entendimiento del secreto como valioso instrumento competitivo del que dispone el empresario en la liza concurrencial, así como la vinculación de su tutela al interés del consumidor y de la entera colectividad en el aseguramiento de que los operadores económicos acuden al mercado armados exclusivamente con su propia eficiencia confluyen en una nueva perspectiva, que incide, a los efectos que nos interesan, en dos elementos fundamentales, a saber, el objeto material y las acciones típicas. Las conclusiones alcanzadas en sede de bien jurídico cobran una extraordinaria relevancia en la interpretación de estos dos elementos, puesto que, proyectadas al objeto y al medio comisivo, permitirán determinar cuándo esas conductas devienen ilícitas y, en esa medida, serán básicamente dichos elementos los que delimitarán el ámbito de lo punible, con independencia de que puedan plantearse otros problemas.

XXVI

A tenor de todo lo expuesto, el secreto empresarial se configura como una noción genérica, omnicomprendiva de las categorías relativas al secreto industrial y al secreto comercial, incluidas también las informaciones atinentes al sector organizativo o financiero. Así pues, el secreto empresarial aglutina heterogéneas informaciones concernientes a los diversos ámbitos o

parcelas que componen la actividad empresarial. La inclusión de toda esta información, incluida la relativa a ese último grupo especialmente conflictivo, en el contenido del concepto de secreto, se subordina, únicamente, al cumplimiento de los requisitos configuradores en estos conocimientos, experiencias o ideas. Así pues, el concepto de secreto adoptado se proyecta al objeto y, así, su ámbito resulta conformado por los distintos objetos enumerados integrantes del secreto industrial y por las informaciones reservadas propias del secreto comercial, cuya configuración se lleva a cabo de modo residual a la del secreto industrial.

XXVII

El secreto industrial engloba conocimientos relativos a la fabricación de un determinado producto, a la aplicación de un determinado procedimiento, a la producción y prestación de un determinado servicio y, en fin, cualquier información relacionada con el ámbito técnico-productivo de la actividad económica. Su ámbito resulta conformado por los distintos objetos integrantes del secreto industrial, como los descubrimientos científicos, invenciones patentables no patentadas e invenciones no patentables, dibujos y modelos industriales, aplicaciones industriales, prácticas manuales, ensayos e investigaciones, programas de ordenador).

XXVIII

El **secreto comercial**, definido residualmente respecto al industrial, incluye información atinente a la esfera estrictamente comercial, a la organizativa y a la financiera de la empresa. Así, comprende listas de proveedores y clientes, estrategias financieras, planes publicitarios, técnicas de venta, programas de marketing. La inclusión de cualquier información, y también la relativa a ese grupo especialmente conflictivo, que suele concernir a cuestiones atinentes

a la propia organización interna de la empresa (situación financiera, proyecto de celebrar un contrato, estudios de mercado), en el objeto del secreto comercial o, en suma, del secreto empresarial, se subordina al cumplimiento de los requisitos configuradores en estos conocimientos, experiencias o ideas.

XXIX

El empleo de los requisitos configuradores como criterio delimitador del concepto penal de secreto, que se proyecta sobre el contenido de su objeto, ha permitido incluir esos discutidos conocimientos, que, desde una perspectiva apriorística, sí revisten los requisitos analizados y, en concreto, el relativo al valor económico o competitivo de la información, cuya interpretación se verifica en términos relativos. Así pues, basta la concurrencia de los requisitos configuradores, como criterio que ejerza la restricción necesaria para que la información adquiera relevancia jurídico-penal.

XXX

Las diversas modalidades atentatorias de los secretos se hallan, en su mayoría, expresamente previstas por el código penal en los preceptos reguladores de la materia objeto de estudio (así, por ejemplo, la acción de apoderamiento, la relativa al control audiovisual clandestino y control ilícito de señales de comunicación, la revelación, difusión o cesión y, por último, la utilización). Otras, sin embargo, se encuentran todavía ayunas de referencia legal en estos delitos (así, la reproducción, el “apoderamiento” abusivo y la destrucción, alteración o inutilización de los secretos). Resulta incontrovertible que, con la incorporación **ex novo** de alguna de estas acciones y con la nueva redacción otorgada a otras de ellas ya previstas en

el anterior código, se ha avanzado notablemente y se ha logrado acompasar el derecho penal a las características de modernidad, globalidad e informatización de la actual realidad económica y empresarial. Ahora bien, también es cierto que la protección de los secretos de empresa adolece de bondad sistemática y que el desacierto en el orden de las acciones hace perder matices y perfiles, genera lagunas legales y evidencia dislates valorativos.

XXXI

Por lo que se refiere a la primera de las modalidades atentatorias, que se integra por el **acceso ilícito** a la información, se prevén expresamente dos conductas distintas, a saber, el apoderamiento y la interceptación.

XXXII

El **apoderamiento** comprende conductas de captación intelectual, sin desplazamiento físico (apoderamiento de datos) y conductas de apoderamiento físico subrepticio de los objetos que incorporan el secreto (apoderamiento de documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo). Así pues, **de lege lata** esta modalidad permite abrazar todos aquellos objetos en los que puede quedar plasmada la información empresarial de carácter secreto.

XXXIII

La interceptación o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción abraza las conductas reconducibles a la idea de control auditivo (grabación, escucha o interceptación de comunicaciones habladas) o visual (filmación-captación de imágenes), así como los

comportamientos de interceptación, grabación o reproducción ilícita de otros medios de comunicación, como las comunicaciones por telefax o a través de una red informática, ya sea de área local (**intranet**) o de área amplia (como, por ejemplo, Internet). Con su previsión, se ha afrontado, satisfactoriamente, el espionaje empresarial acometido por medios informáticos. En este caso, la deficiencia más importante se produce, por lo que se refiere a la conducta de interceptación en una intranet, en los supuestos de extralimitación, que, también resultan problemáticos en el ámbito del apoderamiento.

XXXIV

Frente a las conductas analizadas (apoderamiento e interceptación), que, de modo expreso, aparecen recogidas en el código, no se prevén otras modalidades de ataque, que, estrechamente vinculadas a los abusos informáticos, pueden, de igual forma, incidir sobre el secreto de empresa, como, por ejemplo, la reproducción, el “apoderamiento” abusivo y la destrucción, alteración o inutilización del secreto.

XXXV

La conducta de **reproducción** comprende, esencialmente, la copia de la información acometida por medios informáticos, a fin de procurarse certeramente el contenido del secreto, conformándose como una modalidad de ataque de entidad y desvalor distinto --en algunos casos, al menos— a los de la conducta de acceso. El código, sin embargo, no contempla la conducta de reproducción como modalidad de ataque independiente. Únicamente aparece contemplada en la modalidad de interceptación, en cuya regulación el código sanciona dicha acción y cualquier reproducción posterior. Por el contrario, no aparece prevista en la modalidad de apoderamiento, pese a lo cual, en la medida en que la conducta de reproducción siempre implicará

una conducta previa de acceso, podrá formar parte de su ámbito de tutela, aunque, sin duda, ***el apoderamiento puede constituir un medio comisivo menos grave*** que la reproducción.

XXXVI

El “***apoderamiento***” ***abusivo*** se integra por el acometido con autorización para acceder a los datos o adueñarse de los soportes, pero abusando de dicha autorización --o sea, no en la forma en que debiera hacerlo, sino dándole un uso distinto--. Esta modalidad atentatoria reconducible al abuso de funciones o a la extralimitación, no se halla prevista ni en el ámbito del apoderamiento ni en el de la interceptación.

XXXVII

Los comportamientos de ***destrucción***, ***alteración*** o ***inutilización***, como modalidades de ataque sobre el secreto de empresa, tampoco se hallan expresamente previstos en la regulación de estos delitos. Así, para subsanar esta laguna debe acudir a la aplicación de otros preceptos y, en concreto, al tipo regulador del sabotaje informático, contemplado en el art. 264.2 CP. Sin embargo, la propia ubicación sistemática de los daños informáticos en los delitos contra el patrimonio y la compleja identificación del bien jurídico protegido entorpecen su idoneidad para reprimir estas modalidades de ataque sobre el objeto material de los delitos reguladores del secreto de empresa y acaban procurando al bien jurídico protegido por estos últimos una tutela asistemática.

XXXVIII

La **revelación, difusión o cesión** del secreto, constituye otra de las modalidades de acción típica, que se halla expresamente contemplada en los delitos relativos a la protección del secreto empresarial, tanto si el sujeto ha accedido ilícitamente a la información o legítimamente, pero con deber de guardar reserva. En la interpretación de estos tres términos no se han podido encontrar criterios unívocos que deslinden con claridad sus respectivos ámbitos de aplicación, de modo que asumen una significación análoga o equivalente, que permite cubrir **de lege data** cualquier posible laguna pero que entorpece la exégesis de estas modalidades, al forzar una inteligencia distinta para cada uno de ellos.

IXL

La **utilización** del secreto, que constituye la última de las modalidades atentatorias, supone el aprovechamiento económico del secreto, lo que determina el rechazo de una interpretación amplia del término, como concepto o modalidad omnicomprensiva de la anterior acción. Esta modalidad se halla expresamente recogida en el art. 279.2 CP. La técnica empleada en su configuración (regulación en un único precepto con la modalidad de revelación, difusión y cesión; ausencia de remisión a los sujetos y, especialmente, determinación de la pena a partir de la del tipo de la revelación) han suscitado dispares pronunciamientos doctrinales sobre su condición de **modalidad atentatoria privilegiada** y, por tanto, dependiente de la conducta básica de revelación del secreto por quien ha accedido a él legítimamente, pero con deber de guardar reserva o su calificación como **tipo autónomo**. A nuestro parecer, esta última opción se ha estimado preferible, ya que su entendimiento como acción típica autónoma autoriza su aplicación sin necesidad de hacer referencia al tipo previsto en el art. 279.1 CP y, por tanto, como modalidad diversa al acceso y a la revelación. Ello, a su vez,

permite salvar indeseables lagunas legales (como la utilización del secreto por quien accede a él ilícitamente) y explicar una más adecuada gradación en la penalidad.

XL

Esta delimitación del ámbito de lo punible desde el examen de las modalidades típicas ha desvelado, **de lege lata**, algunos vacíos legales y ciertas consecuencias disfuncionales. Esta conclusión crítica alcanzada reclama, pues, en buena lógica, esbozar una sucinta propuesta **de lege ferenda**. El modelo de sistemática postulable más adecuado, desde el punto de vista de las acciones típicas, no implica modificar la naturaleza que, en el código, asumen estos delitos (apoderamiento, interceptación, difusión, revelación, cesión y utilización) y descansa en la incriminación de las cuatro modalidades atentatorias analizadas, a saber, el acceso, la destrucción, alteración e inutilización, la comunicación y la explotación.

BIBLIOGRAFÍA UTILIZADA

- ALBAMONTE, A., "L'oggetto della tutela penale del reato di rivelazione di segreti scientifici o industriali", en **La Giustizia Penale**, II, 1974.
- ALESSANDRI, A., **Riflessi penalistici della innovazione tecnologica**, Milano, 1984.
- ÁLVAREZ MARTÍNEZ, C. y VIZMANOS, T.M., **Comentarios al Código Penal**, 2ª ed., tomo II, Madrid, 1853.
- APARICIO ACOSTA, F. M., "Donde reside el valor", en **El País**, miércoles 10 de mayo de 2000.
- ARE, M., voz: "Beni immateriali (Diritto privato)", en **Enciclopedia del Diritto**, T. V, Milano, 1959.
- ARIANS, K., "Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in der Bundesrepublik Deutschland", en OEHLER (Hrsg), **Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in den Ländern der Europäischen Gemeinschaft sowie in Österreich und der Schweiz**, I, 1978.
- ARROYO ZAPATERO, L., "Actualidad político criminal del derecho penal económico en España", en ARROYO ZAPATERO, L./TIEDEMANN, K., **Estudios de derecho penal económico**, Universidad de Castilla-La Mancha, 1994.
- ARROYO ZAPATERO, L./GARCÍA RIVAS, N., "Comentario a la Ley Orgánica 6/1987, de 11 de noviembre, por la que se modifica la Sección III del Capítulo IV, Título XIII, Libro II del Código penal", en BERCOVITZ RODRÍGUEZ-CANO, R. (Coord.), **Comentarios a la ley de propiedad intelectual**, Madrid, 1989.
- "Protección penal de la propiedad intelectual", en ARROYO ZAPATERO, L./TIEDEMANN, K., **Estudios de derecho penal económico**, Universidad de Castilla-La Mancha, 1994.
- ASCARELLI, T., en **Iniciación al estudio del Derecho Mercantil**, (trad. por VERDERA, E.), Barcelona, 1964.
- **Teoría de la concurrencia y de los bienes inmateriales**, trad. de E. VERDERA y L. SUÁREZ-LLANOS, Barcelona, 1970.

ASÚA BATARRITA, A., “El daño patrimonial en la estafa de prestaciones unilaterales (subvenciones, donaciones, gratificaciones). La teoría de la frustración del fin”, en **ADPCP**, 1993.

AUTERI, P., “Il segreto industriale”, en **Il segreto nella realtà giuridica italiana (Atti del Convegno Nazionale, Roma, 26-28 ottobre, 1981)**, Padova, 1983.

BAJO FERNÁNDEZ, M., **Derecho penal económico aplicado a la actividad empresarial**, Madrid, 1978.

- “Los delitos contra el orden socioeconómico en el Proyecto de Código Penal”, en **RDFUCM, La reforma del derecho penal**, nº 58, monográfico, nº 3, 1980.
- “Política criminal y reforma penal. Delitos patrimoniales económicos”, en AA VV, **Política criminal y reforma penal, Homenaje a la memoria del Prof. Dr. D. Juan del Rosal**, Madrid, 1993.
- “Derecho penal económico: desarrollo económico, protección penal y cuestiones político/criminales”, en **Hacia un derecho penal económico europeo. Jornadas en honor del Profesor Klaus Tiedemann**, Madrid, 1995.

BAJO FERNÁNDEZ, M./SUÁREZ GONZÁLEZ, C., en BAJO FERNÁNDEZ, M./PÉREZ MANZANO, M./SUÁREZ GONZÁLEZ, C., **Manual de derecho penal. Parte Especial. Delitos patrimoniales y económicos**, Madrid, 1993.

BAJO FERNÁNDEZ, M./BACIGALUPO, S., **Derecho penal económico**, Madrid, 2001.

BARCELÓ, M., “La nueva sociedad del conocimiento”, en AA VV, **La sociedad del conocimiento**, Barcelona, 1998.

- “Cataluña y la economía digital”, en **El País**, 2/Cataluña, sábado 13 de mayo de 2000.

BARCELLONA, P., **Il capitale como puro spirito**, Roma, Riuniti, 1990.

BARJONET, A., “Nature et perspectives de l’automation”, en **France Nouvelle**, nº 750 y 751, 1960.

BAYLOS CORROZA, H., en “Fundamento filosófico y social de la propiedad industrial”, en **I Cursillo sobre propiedad industrial**, celebrado en Madrid, octubre-diciembre 1966, Barcelona, 1969.

- **Tratado de Derecho Industrial**, 2ª ed. actualizada, Madrid, 1993.

BERCOVITZ, A., “La formación del derecho de la competencia”, en 2 **ADI**, 1975.

- “La competencia desleal”, en ***Derecho de los Negocios***, nº 20, 1992.
- BERCOVITZ RODRÍGUEZ-CANO, R. “Comentario al artículo 1º”, en BERCÓVITZ RODRÍGUEZ-CANO, R. (Coord), ***Comentarios a la ley de propiedad intelectual***, Madrid, 1989.
- BERDUGO GÓMEZ DE LA TORRE, I., “ La tutela de la competencia en la Propuesta de Anteproyecto del Nuevo Código penal”, en ***La reforma penal: delitos socioeconómicos***, Madrid, 1985.
- BONDÍA ROMÁN, F., ***La propiedad intelectual. Su significado en la sociedad de la información***, Madrid, 1988.
- BOURGEOIS, M., “La protection juridique de l’information confidentielle économique: étude de droits québécois et français”, en ***Rev. Int. Dr. Comp.***, nº 1, 1988.
- BRICOLA, F., “Teoria generale del reato”, en Novissimo Digesto Italiano, vol. XIX, Milano, 1973.
- “La riscoperta delle «pene private» nell’ottica del penalista”, en ***Politica del Diritto***, XVI, n.1, marzo 1985.
 - “Lo statuto penale dell’impresa: profili costituzionali”, en DI AMATO, A., ***Tratatto di Diritto Penale dell’Impresa***, vol. I, Padova, 1990.
- BROSETA PONT, M., ***Manual de Derecho Mercantil***, 9.ª ed., Madrid, 1991.
- BUSTOS RAMÍREZ, J., ***Manual de derecho penal, Parte Especial***, 2ª ed., Barcelona, 1991.
- CALLMANN, R., ***The Law of Unfair Competition, Trademarks and Monopolies***, (4 ed. por ALTMAN, L.), Deerfield, Illinois, Callaghan, 1981, vol. 2.
- CAPELLA HERNÁNDEZ, R., “Estado y derecho ante la mundialización: aspectos y problemáticas generales”, en ***Transformaciones del derecho en la mundialización***, CGPJ, EDJ, 16, Madrid, 1999.
- CAPIZZANO, E., “Contratto di know-how e invenzione non brevettata”, en ***Rivista di diritto industriale***, P.I, 1973.
- CARBONELL MATEU, J.C., ***Derecho penal y principios constitucionales***, Valencia, 1996.
- CARMONA SALGADO, C., ***La nueva ley de propiedad intelectual***, Madrid, 1988.

- CARRASCO ANDRINO, M.M., *La protección penal del secreto de empresa*, Barcelona, 1998.
- CASARES, J., *Diccionario ideológico de la lengua española*, 2 ed., Barcelona, 1971.
- CASTELL BORRÁS, B., *La defensa de la competencia en la C.E.E. Artículo 85 del Tratado de Roma*, Barcelona, 1986.
- CLAVERA, J., "La globalización y la nueva sociedad del conocimiento y de la información: un intento de aproximación desde el punto de vista de la economía", en AA VV, *La sociedad del conocimiento*, Barcelona, 1998.
- COBO DEL ROSAL, M./CARBONELL MATEU, J.C., en AA VV (Coord. VIVES ANTÓN, T.S.), *Derecho penal, Parte especial*, 3ª ed., Valencia, 1990.
- COBO DEL ROSAL, M./VIVES ANTÓN, T.S., *Derecho penal, Parte general*, 5 ed., Valencia, 1999.
- COCCO, G., "La tutela penale del segreto industriale", en DI AMATO, A., *Tratatto di Diritto Penale dell'Impresa*, vol. IV, Padova, 1993.
- CORNISH, W.R., *Intellectual property: patents, copyright, trade marks and allied rights*, London, 1996.
- COROMINAS, J., *Breve diccionario etimológico de la lengua castellana*, 3 ed., Madrid, 1987.
- CORTÉS MARQUÉS, G., *Principios de economía política*, 2.^a ed. ampliada y corregida, Barcelona, 1990.
- CRESPI, A., "Tutela penale del segreto e concorrenza sleale", en *La repressione penale della concorrenza sleale*, Milano, 1966.
- CUELLO CALÓN, E., *Derecho Penal. Parte Especial*, tomo II, Barcelona, 1940.
- CUERDA ARNAU, M.L., "Comentario al artículo 22.8 CP", en VIVES ANTÓN, T.S. Coord., *Comentarios al Código Penal de 1995*, T. I, Valencia, 1996.
- DANNECKER, G. "Der Schutz von Geschäfts- und Betriebsgeheimnissen", en *Der Betriebs-Berater*, 24, 1987.
- DAUB, J., *Die Verletzung von Unternehmensgeheimnissen im deutschen und Us-amerikanischen Recht*, Berlín, 1996.

- DE GISPERT PASTOR, M.T., "La noción de empresa en la Constitución española", en AA VV, **La empresa en la Constitución española**, Pamplona, 1989.
- DE LA CUESTA ARZAMENDI, J.L., "Presupuestos fundamentales del Derecho penal", en **Eguzkilore**, nº 3.
- DEL ROSAL BLASCO, B. "El delito de falsedad en la información social del artículo 290 del Código penal de 1995", en **Empresa y derecho penal (I)**, Madrid, 1999.
- DELMAS-MARTY, M., **Droit Pénal des Affaires. Partie Spéciale: infractions**, Tome 2, 3ª ed., Presses Universitaires de France, Paris.
- DEPENHEUER, F., **Zulässigkeit und Grenzen der Verwertung von Unternehmensgeheimnissen durch den Arbeitnehmer**, Köln, 1995.
- DESSEMONTET, F., **Le savoir-faire industriel. Définition et protection du "know-how" en droit américain**, Genève, 1974.
- DÍAZ Y GARCÍA CONLLEDO, M., "Los derechos de autor y conexos. Su protección penal: cuestiones generales y naturaleza patrimonial, personal o mixta del bien jurídico protegido", en **ADPCP**, 1990.
- DÍEZ PICAZO, L., "Cambio social y evolución jurídica en la sociedad de la información", en **Implicaciones sociojurídicas de las tecnologías de la comunicación**, Citea, Madrid.
- **Fundamentos del derecho civil patrimonial**, vol. III, 4 ed., Madrid, 1995.
 - **Fundamentos del derecho civil patrimonial**, vol. I, Introducción, Teoría del contrato, 5ª ed., Madrid, 1996.
- DÍEZ-PICAZO, L., /GULLÓN, A., **Sistema de derecho civil**, vol.I, Introducción. Derecho de la persona. Autonomía privada. Persona jurídica, 9ª ed., Madrid, 2000.
- DOMÉNECH SÁNCHEZ, R/LLORCA, SIGNES, R., "Las formas de mercado", en SUCH PÉREZ, D/BERENGUER RAMÍREZ, J. (Coord.), **Introducción a la economía**, Madrid, 1994.
- DORMIDO BENCOMO, S., "Tecnologías de la información: reflexiones sobre el impacto social y humanístico", en **Informática y Derecho**, nº 19-22, Mérida, 1998.
- FARRANDO MIGUEL, I., **El deber de secreto de los administradores de sociedades anónimas y limitadas**, Madrid, 1991.

FERNÁNDEZ-MIRANDA Y CAMPOAMOR, A./GARCÍA SANZ, R.M., “Comentario al artículo 20”, en **Comentarios a la Constitución Española de 1978**, (ALZAGA VILLAAMIL, O., dir.), Madrid, 1997.

FERNÁNDEZ DE LA GÁNDARA, L./ CALVO CARAVACA, A.L., “Política y derecho de la competencia en la CEE: una aproximación”, en **Derecho mercantil internacional**, 2ª. ed., Madrid, 1993.

FERNÁNDEZ NOVOA, C., “Reflexiones preliminares sobre la empresa y sus problemas jurídicos”, en **RDM**, nº 95, 1965.

- “La interpretación jurídica de las expresiones publicitarias”, en **RDM**, nº 107, 1968.
- “Reflexiones preliminares sobre la ley de competencia desleal”, en **LL**, 2/1991.
- **El enriquecimiento injustificado en el derecho industrial**, Madrid, 1997.

FERNÁNDEZ SÁNCHEZ, M.T., **Protección penal del secreto de empresa**, Madrid, 2000.

FIKENTSCHER, W., “Las tres funciones del control de la economía (Derecho antimonopolio)”, en **RDM**, nº 172/173, 1984.

FONT GALÁN, J.I., “Competencia desleal y prácticas prohibidas en el marco de la Ley de prácticas restrictivas de la competencia”, en **RDM**, nº 146, 1977.

- “Notas sobre el modelo económico de la Constitución española de 1978”, en **RDM**, nº 152, 1979.
- **Constitución económica y derecho a la competencia**, Madrid, 1987.
- “La crisis de la «relación de competencia» como presupuesto técnico de aplicación de la cláusula general de la competencia desleal”, en **RFDUCM**, 1987.

FONT SEGURA, A., **La protección internacional del secreto de empresa**, Madrid, 1999.

FRIEDMAN, D.D/LANDES, W.M/POSNER, R.A., “Some Economics of Trade Secrets Law”, en **Journal of Economics Perspectives**, Vol. 5, Nº 1, 1991, p. 61.

FRIGNANI, A., “Secretos de empresa (en el Derecho italiano y comparado)”, en **RFDUC**, Curso 1987-1988, Madrid, 1988.

- FROSINI, V., **Cibernética, derecho y sociedad**, Madrid, 1978.
- GALÁN CORONA, E., **Acuerdos restrictivos de la competencia**, Madrid, 1977.
- GALÁN CORONA, E., "Supuestos de competencia desleal por violación de secretos", en **La regulación contra la competencia desleal en la Ley de 10 de enero de 1991**, (BERCOVITZ, A., coord.), Madrid, 1992.
- GALVALDA, C., "Le secret des affaires", en **Mélanges offerts à René Savatier**, Paris, Dalloz, 1965.
- GÁLVEZ MONTES, F.J., "Comentario al artículo 20 CE", en GARRIDO FALLA, F., **Comentarios a la Constitución**, Madrid, 1980.
- GAMM, O.F. v, **Gesetz gegen den unlauteren Wettbewerb**, 3. Auf., Köln/Berlin/Bonn/München,
- **Wettbewerbsrecht. Mit Zugabe- und Rabattrecht sowie mit Nebengesetzen und kartellrechtlichen Vorschriften**, 5. Auf., 1. Halbband, Köln/Berlin/Bonn/München, 1987.
- GARCÍA ARÁN, M., **El delito de hurto**, Valencia, 1998.
- GARCÍA ARÁN, M./LÓPEZ GARRIDO, D., **El Código penal de 1995 y la voluntad del legislador**, Madrid, 1996.
- GARCÍA PABLOS, A., "Informática y Derecho Penal", en **Implicaciones sociojurídicas de la información**, Citema, Madrid.
- GARRIGUES, J., **La defensa de la competencia mercantil**, Madrid, 1964.
- "La propiedad industrial y la empresa", en **ADI**, 1977.
- GHIDINI, G., **Slealtà della concorrenza e costituzione economica**, Padova, 1978.
- GIMENO OLCINA, L., "Algunos problemas de la Ley de Competencia Desleal", en **LL**, 1993, T. 2.
- GIRÓN TENA, J., "Competencia ilícita y derecho a la empresa. Interpretación de nuestro derecho positivo", en **Revista de derecho privado**, 1944; **Estudios de Derecho Mercantil**, Madrid, 1955.
- GIRÓN TENA, J., "Coloquio-Panel", en **Reforma de la legislación mercantil**, Madrid, 1979.

- GOLDSTEIN, P., *Copyright, Patent, Trademark and Related State Doctrines. Cases and materials on the law of intellectual property*, New York, 1981.
- GÓMEZ BENÍTEZ, J.M., *Curso de Derecho Penal de los negocios a través de casos. Reflexiones sobre el desorden legal*, Madrid, 2001.
- GÓMEZ SEGADÉ, J.A., “En torno al concepto de Know-how”, en *Estudios jurídicos en homenaje a Joaquín Garrigues*, T. II, Madrid, 1971.
- *El secreto industrial (Know-how). Concepto y protección*, Madrid, 1974.
 - “Algunos aspectos de la licencia de Know-How”, en *ADI*, T. 7, 1981.
 - voz “Propiedad industrial (Dº. Mercantil)”, en *EJB*, T.IV,
 - voz “Secreto industrial (D.º Mercantil)”, en *EJB*, T. IV, Madrid, 1995.
- GONZÁLEZ RUS, J.J., “La reforma de los delitos económicos y contra el patrimonio. Consideraciones críticas”, en *EPCr.*, XVII, 1993-1994.
- en AA VV, (COBO DEL ROSAL, M., Dir.), *Curso de derecho penal español, Parte especial, I*, Madrid, 1996.
- GROIZARD y GÓMEZ DE LA SERNA, A., *El Código Penal de 1870, Concordado y Comentado*, tomo V, Burgos, 1870-1899.
- GUILLAMAUD, J., *Cibernética y lógica dialéctica*, Madrid, 1971.
- GUINARTE CABADA, G., *La tutela penal de los derechos de propiedad industrial*, Madrid, 1988.
- “Consideraciones político-criminales en torno a la competencia desleal”, en *EPCr.*, XV, 1990-1991.
- GUTIÉRREZ FRANCÉS, M.L., “Notas sobre la delincuencia informática: atentados contra la <información> como valor económico de empresa”, en ARROYO ZAPATERO, L./TIEDEMANN, K., *Estudios de derecho penal económico*, Universidad de Castilla-La Mancha, 1994.
- HARTE-BAVENDAMM, H., “Schutz von Geschäfts- und Betriebsgeheimnis”, en GLOY (Hrsg), *Handbuch des Wettbewerbsrechts*, 2. Auf., München, 1997.
- HASSEMER, W., “Il bene giuridico nel rapporto di tensione tra costituzione e diritto naturale”, en *Dei delitti e delle pene*, 1984, nº 1.
- HEFERMEHL, W., en BAUMBACH/HEFERMEHL, *Wettbewerbsrecht. Gesetz gegen den unlauteren Wettbewerb, Zugabeverordnung, Rabattgesetz und*

- Nebengesetze**, por W. Hefermehl, originalmente a cargo de A. Baumbach, 19 Auf., München, 1996; 21. Auf., 1999.
- HORMÁZABAL MALARÉE, H., **Bien jurídico y Estado social, democrático y de derecho**, Barcelona, 1991.
- HULL, J., **Commercial secrecy: Law and Practice**, London, 1998.
- JAGER, M.F., **Trade Secrets Law by Melvin F. Jager**, Clark Boardman Callaghan, New York, 1993, Vol. 1.
- JASO ROLDÁN, J., en ANTÓN ONECA, J./RODRÍGUEZ MUÑOZ, J.A., **Derecho penal, Parte especial**, T. II, Madrid, 1949.
- JORGE BARREIRO, A., “Descubrimiento y revelación de secretos. Un estudio de derecho penal español (arts. 497-499 del C.p. español)”, en **Revista de derecho público**, nº 87, 1982.
- KALBHEN, U./KRÜCKEBERG, F./REESE/J., **Las repercusiones sociales de la tecnología informática**, Madrid, 1983.
- KÖHLER, H., **Gesetz gegen den unlauteren Wettbewerb**, München, 1995.
- KOHLER, J., **Deutsches Patentrecht**, Mannheim-Straßburg, 1878.
- KRAGLER, P., “Das Strafverfahren wegen privater Wirtschaftsspionage; ausgewählte Fragen zur strafprozessualen Problematik von Verfahren nach § § 17 ff. UWG”, en **wistra**, 1, 1983.
- LACRUZ BERDEJO, J.L., **Elementos de derecho civil, III, Derechos reales**, vol.1, Posesión y propiedad, 3 ed. revisada, Barcelona, 1991.
- LACRUZ BERDEJO, J.L./LUNA SERRANO, A./RIVERO HERNÁNDEZ, F., **Elementos de derecho civil, I. Parte general del derecho civil**, vol.3, El derecho subjetivo, Barcelona, 1990.
- LAMPE, E.J., “La protección jurídico-penal de la competencia económica en el Anteproyecto de Código Penal español de 1983”, en **La reforma penal: delitos socio-económicos**, Madrid, 1985.
- LANDECHO VELASCO, C.M./MOLINA BLÁZQUEZ, C., **Derecho penal español, Parte especial**, Madrid, 1996.
- LANDROVE DÍAZ, G., “Descubrimiento y revelación de secretos”, en AA VV, **III Jornadas de profesores de Derecho Penal**, Santiago de Compostela, 1976.
- LARENZ, K., **Metodología de la ciencia del derecho**, Barcelona, 1994.

- LAVER, M., *Los ordenadores y el cambio social*, Madrid, 1982.
- LOBATO GARCÍA, M., “Sobre la «usucapio libertatis» de los bienes inmateriales”, en *Revista de derecho privado*, 1990.
- LOSANO, M.G., *Curso de informática jurídica*, Madrid, 1987.
- LUKES, R., *Schutz von Betriebs- und Geschäftsgeheimnissen in ausgewählten EG-Staaten*, Berlín, 1986.
- LLOBREGAT HURTADO, M.L., *Aproximación al concepto de secreto empresarial en Derecho Español y Derecho Norteamericano*, Barcelona, 1999.
- MADRENAS I BOADAS, C., *Sobre la interpretación de las prohibiciones de publicidad engañosa y desleal. La parcialidad de la publicidad y los costes de la competencia*, Madrid, 1990.
- MAGNIN, F., *Know-how et propriété industrielle*, Paris, Libraires techniques, 1974, nº 26.
- MARTÍNEZ PÉREZ, C., “Los delitos relativos al mercado y a los consumidores en el proyecto de código penal de 1992”, en *EPCr.*, XVI, 1992-1993.
- en AA VV, (Coord. VIVES ANTÓN, T.S.), *Comentarios al Código Penal de 1995*, Volumen II, Valencia, 1996.
 - *Derecho penal económico, Parte general*, Valencia, 1998.
 - *Derecho penal económico, Parte especial*, Valencia, 1999.
- MARTOS NÚÑEZ, J.A., *Derecho penal económico*, Madrid, 1987.
- MASCAREÑAS, C.E., en *Los delitos contra la propiedad industrial*, Barcelona, 1960.
- MASSAGUER FUENTES, J.J., *El contrato de licencia de know-how*, Barcelona, 1989.
- “Aproximación sistemática general al Derecho de la competencia y de los bienes inmateriales”, en *RGD*, nº 544-545, 1990.
 - “El enjuiciamiento *antitrust* de los acuerdos de licencia de patente y de licencia de *know-how* tras la reforma del derecho español de defensa de la competencia”, en *La Ley*, 2/1992, Madrid, 1992,
 - “Inducción a la infracción contractual”, en *ADI*, XV, 1993.

- “Los secretos industriales y comerciales y su transmisión: régimen jurídico”, en FONT GALÁN, J.I./NAVARRO CHINCHILLA, J.J./VÁZQUEZ GARCÍA, R.J., ***Derecho de la propiedad industrial, Cuadernos de Derecho y Comercio***, Monográfico, 1994.
 - voz “Competencia desleal (D.º Mercantil)”, en ***EJB***, Vol. I.
 - ***Los derechos de propiedad industrial e intelectual ante el derecho comunitario: libre circulación de mercancías y defensa de la competencia***, CEFI, Madrid, 1995.
 - ***Comentario a la Ley de Competencia Desleal***, Madrid, 1999.
- MATILLA ALEGRE, R., “La noción de competencia y la orientación fundamental de la Ley española sobre represión de prácticas restrictivas de competencia”, en ***Revista General de Legislación y Jurisprudencia***, T. 247, 1979.
- MAZZACUVA, N., “Tutela penale del segreto e controllo del processo produttivo”, en ***Rivista Giuridica del Lavoro***, T. IV, 1977.
- ***La tutela penale del segreto industriale***, Milano, 1979.
- McMANIS, Ch. R., ***The law of unfair trade practices in a nutshell***, St. Paul, Minn., 1982.
- MENÉNDEZ MENÉNDEZ, A., ***Constitución, sistema económico y derecho mercantil***, Universidad Autónoma de Madrid, Madrid, 1982.
- ***La competencia desleal***, Madrid, 1988.
- MERCADO PACHECO, P., “El «Estado comercial abierto». La forma de gobierno de una economía desterritorializada”, en ***Transformaciones del derecho en la mundialización***, CGPJ, EDJ, 16, Madrid, 1999.
- METZLER R., ***Konsequenzen neuartiger Erscheinungsformen des wirtschaftlichen Wettbewerbes für den strafrechtlichen Schutz von Geschäfts- und Betriebsgeheimnissen im Rahmen der §§ 17ff UWG***, München, 1990.
- MILGRIM, R. M., ***Milgrim on trade secrets***, Vol. I, New York, Matthew Bender, 1967-1991.
- ***Milgrim on licensig***, Vol. I, New York, Matthew Bender, 1997.
- MIR PUIG, S., ***El Derecho penal en el Estado social y democrático de derecho***, Barcelona, 1994.

- **Derecho penal, Parte general**, 4 ed., Barcelona, 1996.

MOLINA BLÁZQUEZ, C., "La criminalización de la competencia desleal en el Proyecto de Código Penal de 1992", en **PJ**, nº 28, 1992.

MOLINER, M., **Diccionario de uso del español**, 2ª ed. Madrid, 1998.

MÖHRENSCHLAGER, M., "Das neue Computerstrafrecht", en **wistra**, 4, 1986.

MONEREO PÉREZ, L., "El Derecho social y del trabajo en el mundo de la tercera revolución industrial", en **Transformaciones del derecho en la mundialización**, CGPJ, EDJ, 16, Madrid, 1999.

MORALES PRATS, F., **La tutela penal de la intimidad: privacy e informática**, Barcelona, 1984.

- "Garantías penales y secreto sumarial", en **LL**, 1985.
- "Privacy y reforma penal: la Propuesta de Anteproyecto de Nuevo Código Penal de 1983", en **Documentación jurídica**, núm. 37/40, Monográfico dedicado a la Propuesta de Anteproyecto del Nuevo Código Penal, vol. 1, Madrid, 1983.
- "Presupposti politico-criminali per una tutela penale della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo)", en **Il Diritto dell'Informazione e dell'Informatica**, n. 2, maggio-agosto, 1986.
- "Adecuación social y tutela penal del honor: perspectiva despenalizadora", en **RFDUG**, nº 12, 1987.
- "Problemática jurídico-penal de las libertades informáticas en España tras diez años de vigencia de la Constitución de 1978", en **EPCr.**, XII, 1989.
- "Técnicas de tutela penal de los intereses difusos", en **Intereses difusos y derecho penal**, CDJ, CGPJ, XXXVI, Madrid, 1994.
- "Protección de la intimidad: delitos e infracciones administrativas", en **La protección del derecho a la intimidad de las personas (fichero de datos)**, CDJ, CGPJ, 1997.
- "Pornografía infantil e Internet: la respuesta en el Código penal español", en **Problemática jurídica en torno al fenómeno de Internet**, CDJ, CGPJ, Madrid, 2000.

- MORALES PRATS, F./GARCÍA ALBERO, R., “Comentario a los delitos contra la libertad e indemnidad sexual”, en AA VV, (QUINTERO OLIVARES, Dir.), **Comentarios a la parte especial del derecho penal**, Pamplona, 1999.
- MORALES PRATS, F./MORÓN LERMA, E., en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios a la parte especial del derecho penal**, Pamplona, 1999.
- MORENO CÁNOVAS, A./RUIZ MARCO, F., **Delitos socioeconómicos**, Zaragoza, 1996.
- MORENO Y BRAVO, E., en AA VV, (BACIGALUPO, E., Dir.), **Curso de derecho penal económico**, Madrid, 1998.
- MORÓN LERMA, E., **Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red**, Pamplona, 1999.
- MUÑOZ CONDE, F., “La ideología de los delitos contra el orden socioeconómico en el Proyecto de Ley Orgánica de Código Penal”, en **CPC**, nº 16, 1982.
- **Derecho penal. Parte especial**, Sevilla, 1976; 8ª ed., Valencia, 1991.
 - “Delincuencia económica: estado de la cuestión y propuestas de reforma”, en **Hacia un derecho penal económico europeo. Jornadas en honor del Profesor Klaus Tiedemann**, Madrid, 1995.
- MUTTI, P., “Segreti scientifici o industriali (rivelazione di)”, en **Digesto delle Discipline Penalistiche**, vol. XIII, UTET, Torino, 1997.
- NASTELSKI, N., “Der Schutz des Betriebsgeheimnisses”, en **GRUR**, I, 1957.
- NATHAN, D., “Trade Secrets in the Area of High Technology”, en **Eur. Intell. Prop. R.**, Vol. 13, Issue 8, 1991.
- NIEMEYER, J., “Geheimnisverletzungen”, en MÜLLER-GUGENBERGER (Hrsg), **Wirtschaftsstrafrecht**, Münster, 1992.
- NORA, S/MINC, A., **La informatización de la sociedad**, FCE España, Madrid, 1980.
- NORDEMANN, W., **Wettbewerbs- und Markenrecht**, 6. Auf., Baden-Baden, 1995.
- NOTE, en “Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy”, en **Harvard Law Review**, vol. 106, nº 2, 1992 .
- NOVOA MONREAL, E., **Derecho a la vida privada y libertad de información. Un conflicto de derechos**, Madrid, 1989.

- OCTAVIO DE TOLEDO Y UBIETO, E., "Algunas reflexiones sobre el tratamiento jurídico del secreto profesional", en **LL**, 1983.
- OCTAVIO DE TOLEDO Y UBIETO, E./HUERTA TOCILDO, S., **Derecho penal, Parte general. Teoría jurídica del delito**, 2ª ed., Madrid, 1986.
- OTAMENDI RODRÍGUEZ-BETHENCOURT, J.J., **Comentarios a la ley de competencia desleal**, Pamplona, 1994.
- OTERO LASTRES, J.M., "La nueva Ley sobre Competencia Desleal", en **LL**, 1991, T.4.
- PACHECO, J.F., **El Código Penal Concordado y Comentado**, tomo III, 5ª. ed. corregida y aumentada, Madrid, 1881.
- PALIERO, C.E., "La sanción administrativa como medida moderna en la lucha contra la criminalidad económica", **Hacia un derecho penal económico europeo. Jornadas en honor del Profesor Klaus Tiedemann**, Madrid, 1995.
- PANTALEÓN, F., "Artículo 1902", en **Comentario del Código Civil**, Minsiterio de Justicia, II, Madrid, 1991.
- PAZ-ARES, C., "El ilícito concurrencial: de la dogmática monopolista a la política antitrust (Un ensayo sobre el derecho alemán de la competencia desleal)", en **RDM**, nº 159, 1981.
- PEDRAZZI, C., "Odiarne esigenze economiche e nuove fattispecie penali", en **RIDPP**, 1975.
- "Problemi di tecnica legislativa", en **Comportamenti economici e legislazione penale, Atti del Convegno «Arel» del 17 marzo 1978**, Milano, 1979.
 - "El bien jurídico en los delitos económicos", en BARBERO SANTOS, M., (ed.) **La reforma penal: delitos socio-económicos**, Madrid, 1985.
- PÉREZ LUÑO, A.E., **Nuevas tecnologías, sociedad y derecho**, Madrid, 1987.
- PETERSON, G.R., "Trade Secrets in an Information Age", en **Houston Law Review**, vol. 32, n.2, 1995.
- PFISTER, B., **Das technische Geheimnis <know-how> als Vermögensrecht**, München, 1974.
- POINTET, P.J., "Función de la propiedad industrial en el desarrollo económico de los países", en **I Cursillo sobre propiedad industrial**, celebrado en Madrid, octubre-diciembre 1966, Barcelona, 1969.

- POLAINO NAVARRETE, M., “Descubrimiento y revelación de secretos”, en AA VV (Dir. COBO DEL ROSAL), **Manual de Derecho Penal (Parte Especial)**, Madrid, T.I., 1993.
- PORTELLANO DÍEZ, P., **La imitación en el Derecho de la competencia desleal**, Madrid, 1995.
- **Deber de fidelidad de los administradores de sociedades mercantiles y oportunidades de negocio**, Madrid, 1996.
 - “Los nuevos delitos contra la propiedad industrial. Reflexiones de un mercantilista”, en **RDM**, nº 221, 1996.
 - “Protección de la información no divulgada”, en **Los derechos de propiedad intelectual en la organización mundial del comercio**, T. I, Madrid, 1997.
- PORTILLA CONTRERAS, G., “Principio de intervención mínima y bienes jurídicos colectivos”, en **CPC.**, nº 39, 1989.
- POSNER, R., “Trade secret misappropriation: a cost-benefit response to the fourth amendment analogy”, en **Harvard Law Review**, vol. 106, 1992, nº2.
- PRATS CANUT, J.M., “Comentario al artículo 22.8 CP”, en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios al Nuevo Código Penal**, Pamplona, 2ª ed., 2001.
- PREIN, P., **Der Geheimnisschutz im wirtschaftlichen Wettbewerb nach deutschem Recht**, Köln, 1932.
- PUIG PEÑA, F., “Descubrimiento y revelación de secretos”, en **NEJ**, T. VII, Barcelona, 1955.
- **Derecho penal, Parte Especial**, T. IV, Madrid, 1969.
- PULITANÒ, D., “La formulazione delle fattispecie di reato: oggetti e tecniche”, en **Beni e tecniche della tutela penale, Materiali per la riforma del codice**, Milano, 1987.
- QUERALT JIMÉNEZ, J.J., **Derecho penal español, Parte especial**, 2ª ed., Barcelona, 1992.
- QUINTANO RIPOLLÉS, A., **Comentarios al Código penal**, Madrid, 1966.
- **Tratado de la Parte Especial del Derecho Penal**, tomo I, vol. II, Madrid, 1972.

QUINTERO OLIVARES, G., "Economía e instrumentos represivos", en **Papers, Revista de Sociología**, nº 13, Sociedad y delito, Barcelona, 1980.

- "Sobre los presupuestos y limitaciones de la legislación penal española", en **Estudios jurídicos en honor del profesor Octavio Pérez- Vitoria**, T. II, Barcelona, 1983.
- en GÓMEZ BENÍTEZ, J.M. y QUINTERO OLIVARES, G., **Protección penal de los derechos de autor**, Madrid, 1988.
- La justicia penal en España, Pamplona, 1998.
- "Sobre los delitos societarios en el nuevo Código Penal (Cuestiones generales)", en AA VV, ASÚA BATARRITA, A. (Ed.), **Jornadas sobre el nuevo Código Penal de 1995**, Bilbao, 1998.
- "Comentario al título de los delitos contra el patrimonio y contra el orden socioeconómico", en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios a la parte especial del derecho penal**, Pamplona, 1999.
- "Comentario a los artículos 270 a 272 CP", en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios a la parte especial del derecho penal**, Pamplona, 1999.

QUINTERO OLIVARES, G./MORALES PRATS, F./PRATS CANUT, J.M., **Manual de derecho penal, Parte general**, Pamplona, 2000.

RAMELLA, A., "I segreti industriali", en **Rivista penale**, vol. LXIII, 1906.

RAMONET, I., **Un mundo sin rumbo, Crisis de fin de siglo**, Barcelona, 1997.

RAMONET, I., "Nueva economía", **Le Monde diplomatique**, nº 54, abril, 2000.

Real Academia Española, **Diccionario de la lengua española**, 21 ed., Madrid, 1992.

REBOLLO VARGAS, R., **La revelación de secretos e informaciones por funcionario público**, Barcelona, 1996.

REICHMAN, "Computer Programs As Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research", en **Vanderbilt Law Review**, vol. 42, nº 3, 1989.

RODRÍGUEZ DEvesa, J.M., **Derecho penal español, Parte especial**, 8ª ed., Madrid, 1980; 14ª ed. (rev. por SERRANO GÓMEZ, A.), Madrid, 1991.

RODRÍGUEZ RAMOS, L., **Compendio de derecho penal (Parte especial)**, Madrid, 1985.

- RODRÍGUEZ TAPIA, J.M., voz: "Propiedad intelectual (Dº. Civil)", en **EJB**, T. IV., Madrid, 1995.
- ROMEO CASABONA, C.M., **Poder informático y seguridad jurídica**, Madrid, 1987.
- **Nuevas tecnologías, sociedad y derecho**, Madrid, 1987.
- ROJO, A., "Actividad económica pública y actividad económica privada en la Constitución española", en **RDM**, nº 169-170, 1983.
- RUBIO, J., **Introducción al Derecho Mercantil**, Barcelona, 1969.
- SÁNCHEZ BLANCO, A., **Internet. Sociedad, empresa y poderes públicos**, Granada, 2000.
- SÁNCHEZ CALERO, A., "Las costumbres de probidad en la competencia y los secretos industriales", en **Separata de Anales de Moral Social y Económica**, vol. XII, 1966.
- SÁNCHEZ CALERO, F., **Instituciones de Derecho Mercantil**, T.I, Introducción, empresa y sociedades, 18ª. ed., Madrid, 1995.
- SANTAGATA, C., **Concorrenza sleale e interessi protetti**, Napoli, 1975.
- SCHAFHEUTLE, K., **Wirtschaftsspionage und Wirtschaftsverrat im deutschen und schweizerischen Strafrecht**, Freiburg im. Br., 1972.
- SCHMIDT, E., "Bedarf das Betriebsgeheimnisses eines verstärkten Schutzes?", en **Gutachten zum 36. Deutschen Juristentag**, Bd. 1, Berlin und Leipzig, 1931.
- SCHNEIDER, M., **Schutz des Unternehmensgeheimnisses vor unbefugter Verwertung**, Bamberg, 1989.
- SCHÖNFELDER, H., **Deutsche Gesetze, Sammlung des Zivil-, Straf- und Verfahrensrechts**, 98. Auf., München, 1999.
- SCHÜNEMANN, B., "Introducción al razonamiento sistemático en derecho penal", en SCHÜNEMANN, B., (Comp.), **El sistema moderno del derecho penal: cuestiones fundamentales**, Madrid, 1991.
- SCHRICKER, G., "Últimos desarrollos del Derecho de la Competencia Desleal en Europa", en **RGD**, 1993.
- SGUBBI, F., "Tutela penale di «interessi diffusi»", en **La Questione Criminale**, 1975.

SUÁREZ GONZÁLEZ, C., en AA VV (RODRÍGUEZ MOURULLO, G., Dir.), **Comentarios al Código Penal**, Madrid, 1997.

- en AA VV, **Compendio de Derecho Penal (Parte Especial)**, Volumen II, Madrid, 1998.

SEGURA GARCÍA, M.J., **Derecho penal y propiedad industrial**, Madrid, 1995.

- “La protección penal de los derechos integrantes de la propiedad industrial”, en **Empresa y derecho penal (II)**, CDJ, CGPJ, Madrid, 1999.

SERRANO GÓMEZ, A., **Derecho penal, Parte Especial**, Madrid, 1997.

SERRANO-PIEDRECASAS, J.R., “Consideraciones en torno a la protección penal del Know-how”, en **ADPCP**, 1990.

SORDELLI, L., “Il know-how: facoltà di disporre e interesse al segreto”, en **RDI**, P. I, 1986.

STEBUT, D.v, **Geheimnisschutz und Verschwiegenheitspflicht im Aktienrecht**, Köln/Berlin/Bonn/München, 1972,

SUÁREZ-LLANOS, L., **Derecho, economía, empresa. Vol. I. Elementos de teoría general del derecho patrimonial**, Madrid, 1988.

- **Introducción al Derecho Mercantil**, Madrid, 1998.

SUCHANKOVA, M., “Les principes d’Unidroit et la responsabilité précontractuelle en cas de’échec des négociations”, en **RDAL**, nº 6, 1997.

TERCEIRO, J.B., **[Sociedad digit@l](#)**, Madrid, 1996.

TERRADILLOS BASOCO, J., “La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal”, en **RFDUC**, nº 63, 1981.

- **Derecho penal de la empresa**, Madrid, 1995.

TIEDEMANN, K., “Welche strafrechtlichen Mittel empfehlen sich für eine wirksamere Bekämpfung der Wirtschaftskriminalität?”, **Verhandlungen des 49. Deutschen Juristentages**, B. I, T. C, München, 1972.

- “Literaturbericht. Nebenstrafrecht einschliesslich Ordnungswidrigkeitenrecht (Wettbewerbsrecht)”, en **ZStW**, 86, 1974.
- **Wirtschaftsstrafrecht und Wirtschaftskriminalität, Allgemeiner Teil**, T. 1, Hamburg, 1976.

- **Wirtschaftsstrafrecht und Wirtschaftskriminalität, Besonderer Teil**, Hamburg, 1976.
- **Alternativ-Entwurf eines Strafgesetzbuches, Besonderer Teil: Straftaten gegen die Wirtschaft**, Tübingen, 1977.
- "Rechtsnatur und strafrechtliche Bedeutung von technischem Know how", en **Festschrift für Ernst von Caemmerer**, Tübingen, 1978.
- **Poder económico y delito**, Barcelona, 1985.
- "El concepto de derecho económico, de derecho penal económico y de delito económico", en **CPC**, nº 28, 1986.
- **Lecciones de Derecho Penal Económico (Comunitario, español, alemán)**, Barcelona, 1993.

TROLLER, A., "Il segreto industriale nel sistema dei Diritti sui beni immateriali", en **Rivista di Diritto Commerciale**, p. I., 1957.

TROLLER, K., **Manuel du droit suisse des biens immatériels**, Bâle et Francfort-sur-le-Main, 1996.

TUFFNER, M., **Der strafrechtliche Schutz von Wirtschaftsgeheimnissen im Staasschutzrecht und Wettbewerbsrecht**, Diss. Erlangen, 1978.

VALLE MUÑIZ, J.M., "Prólogo al Código Penal ", Pamplona, ed. Aranzadi, 1995.

VALLE MUÑIZ, J.M., "Comentario a los artículos 273 a 277 CP", en AA VV, (QUINTERO OLIVARES, Dir.), **Comentarios a la parte especial del derecho penal**, Pamplona, 1999.

VALLE MUÑIZ, J.M., "Comentario al artículo 287", en AA VV (QUINTERO OLIVARES, Dir.), **Comentarios al Nuevo Código Penal**, Pamplona, 2ª ed., 2001.

VIADA y VILASECA, S., **El Código Penal Reformado de 1870, Concordado y Comentado**, tomo III, 4ª. ed., Madrid, 1890.

VICENT CHULIÁ, F., **Compendio crítico de derecho mercantil**, T. I, Vol. 2º, 3ª ed., Barcelona, 1991.

- "Otra opinión sobre la Ley de Competencia Desleal", en **RGD**, 1993.
- "Poderes públicos y Derecho de la competencia", en **RGD**, 1993.
- **Introducción al Derecho Mercantil**, 12ª. ed., Valencia, 1999.

VIDALES RODRÍGUEZ, C., “Los delitos socioeconómicos en el Código Penal de 1995: La necesidad de su delimitación frente a los delitos patrimoniales”, en ***EPCr.***, XXI, 1998.

VILADÁS JANÉ, C., “Introducción a la delincuencia económica”, en ***Estudios jurídicos en honor del profesor Octavio Pérez- Vitoria***, T. II, Barcelona, 1983.

VIRGÓS SORIANO, M., ***El comercio internacional en el nuevo derecho español de la competencia desleal***, Madrid, 1993.

WENIGER, O., ***La protection des secrets économiques et du savoir-faire (Know-how)***, Lausanne, 1994.