InDret
REVISTA PARA EL ANÁLISIS DEL DERECHO
WWW. INDRET.COM

El delito de daños y el espionaje empresarial: dos ataques compatibles conta la información como bien inmaterial

Carmen Rocío Fernández Díaz
Universidad de Málaga

BARCELONA, ENERO 2018

Abstract

La información empresarial, como bien inmaterial, es objeto de propiedad para su titular, que deberá adoptar las medidas pertinentes para su protección. Hasta aquí se asimila a cualquier bien de naturaleza material. Sin embargo, los ataques a la información presentan ciertas peculiaridades, derivadas de su carácter intangible, que hacen que sean posibles supuestos de captación y utilización, de forma simultánea a su destrucción, por ser susceptibles de reproducción, a diferencia de lo que ocurre con los bienes materiales. Ello hace que puedan darse casos en los que estemos exclusivamente ante un delito de espionaje empresarial, otros en los que solo se dé un delito de daños o que tengan lugar ambos a la vez. La solución a la que se llegue dependerá principalmente de la dimensión subjetiva del autor del delito, como elemento que permitirá determinar el fin que perseguía con su conducta y, por tanto, el caso ante el que nos encontramos. El presente trabajo trata las peculiaridades de ambos delitos relacionadas con el carácter inmaterial de la información y con los problemas que suscita su regulación, estudiando la casuística posible que puede darse entre el espionaje y los daños, a efectos de poder deslindar correctamente cuándo se produce cada caso.

Die Geschäftsinformationen als immaterielles Gut sind Eigentum ihres Inhabers, der geeignete Maßnahmen zu ihrem Schutz ergreifen muss. In dieser Hinsicht haben sie dieselbe Natur wie andere Güter materieller Natur. Allerdings weisen die Angriffe auf die Informationen wegen der immateriellen Natur der Letzteren einige Besonderheiten auf. Im Gegensatz zu den materiellen Gütern können solche Informationen auf Grund ihrer immateriellen Natur aufgenommen und benutzt werden. Deshalb gibt es erstens Kontstellationen, in denen ausschließlich eine Straftat der Wirtschaftsspionage vorliegt, zweitens gibt es Konstellationen, bei denen nur eine Sachbeschädigung vorliegt, sowie drittens Konstellationen, in denen beide Straftaten vorliegen. Die Lösung hängt hauptsächlich von der subjektiven Dimension des Straftäters als ein Merkmal ab, das den von seinem Verhalten verfolgten Zweck bestimmt. Diese Arbeit erörtert die Besonderheiten beider Straftaten im Zusammenhang mit der Immaterialität von Informationen sowie aus ihre Regulierung entstehende Probleme, und untersucht die möglichen Fälle, bei denen sich die Frage der Abgrenzung zwischen Spionage und Sachbeschädigung stellt.

Business information, as an intangible asset, is the property of its holder, who must take appropriate measures for its protection. Up to here it is assimilated to any good of material nature. However, attacks on information have certain peculiarities, that derive from their intangible nature, which make possible its capture and use simultaneously with its destruction, as it is susceptible to reproduction, unlike material assets. This means that there may be cases in which we are exclusively dealing with an offense of corporate espionage, others where only a damage crime is committed or those in which both occur at the same time. The solution to be reached will depend mainly on the subjective dimension of the offender, as an element that will determine the purpose that he pursued with his behavior and, therefore, the case before us. The present work deals with the peculiarities of both crimes related to the immaterial nature of the information as well as with the problems that arise from its regulation, and studies the possible casuistry between espionage and damages in order to correctly define when each case occurs.

Titel: Sachbeschädigung und Wirtschaftsspionage: zwei vereinbare Angriffe gegen die Informationen als immaterielles Gut.
Title: Damage crime and corporate espionage: two compatible attacks against information as an intangible asset.

Palabras clave: espionaje empresarial, delito de daños, información, bienes inmateriales, propiedad.
Stichworte: Wirtschaftsspionage, Sachbeschädigung, Informationen, immaterielles Gut, Eigentum.
Keywords: corporate espionage, damage crime, information, intangible assets, property.

Sumario

1. Introducción

Los ataques a la propiedad de un individuo pueden perpetrarse de muy diversas maneras. Ante ellos el Código penal castiga con diferentes delitos los atentados contra ella, ya sea en un sentido material o inmaterial. Si bien el primer tipo de propiedad no suele plantear problemas, por constituir la forma clásica de entenderla, la de carácter inmaterial presenta más peculiaridades.

El presente trabajo aborda dos tipos delictivos, el delito de daños y el de espionaje empresarial, los cuales entrañan una ofensa a la información como bien objeto de protección. Dado el carácter inmaterial y, por tanto, ubicuo, del bien en que se encarna la propiedad, en la práctica el espionaje puede ser compatible e incluso confundible con ataques encuadrables en los tipos de daños, sobre todo en relación con el llamado sabotaje informático.

La seguridad de la información, como elemento de valor económico que es parte de la propiedad de una empresa, puede ser afectada en relación con tres aspectos: su integridad, su disponibilidad y su confidencialidad[1]. Estas tres vertientes de la información pueden ponerse en

[1] INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, «Guía de almacenamiento seguro de la información», 2016, p. 6, *online* en https://www.incibe.es (última visita: 27 de agosto de 2017). En este sentido también, MORÓN LERMA, «Quiebras de la privacidad en escenarios digitales: Espionaje industrial», *Eguzkilore*, (21), 2007, p. 130, *online* en http://www.ehu.eus (última visita: 27 de agosto de 2017); RIBAGORDA GARNACHO, «Seguridad de las tecnologías de la información», *CDJ*, 1996, pp. 312 s., quien estima que un sistema es fiable cuando se satisfacen

riesgo de diferentes maneras, ante las que el Código penal responde diversamente. Así, por un lado, el delito de daños castigaría aquellas conductas que atentan contra la integridad y la disponibilidad de la información, y que podrían darse con su alteración, su borrado, su destrucción o al hacerla inaccesible[2]; por otro lado, con el delito de espionaje se preserva especialmente la confidencialidad de la información, que es la que le otorga su carácter exclusivo. Sin embargo, puede producirse un ataque a sus tres elementos, dándose así un posible concurso de delitos. De manera gráfica podría representarse dicha relación con la siguiente figura.

Fuente: Guía de almacenamiento seguro de la información, 2016
Instituto Nacional de Ciberseguridad (INCIBE)

Un ataque a las zonas celeste y naranja de la figura constituiría un delito de daños exclusivamente (borrado, dañado, alteración, destrucción, bloqueo o inutilización de la información), mientras que, si este tuviera lugar en la zona rosa, solo se daría espionaje (apoderamiento ilegítimo o revelación). Sin embargo, podrían darse ambos delitos si la conducta tiene lugar en la zona azul oscuro, donde confluyen los tres elementos, afectando a todos ellos (apoderamiento o revelación de la información y posterior borrado, dañado, alteración, destrucción, bloqueo o inutilización de esta).

Por ello, en el presente trabajo, en primer lugar, se tratará el delito de espionaje empresarial, mediante una aproximación a las cuestiones de interés para el objeto de estudio, como son el bien jurídico protegido, el concepto de secreto de empresa y la cláusula concursal prevista en el tipo. En segundo lugar, aludiré a las diversas modalidades que presentan los delitos de daños a los efectos que aquí interesan, haciendo especial hincapié en aquellos elementos típicos que plantean dudas cuando la información objeto de un posible secreto de empresa sea objeto de estos. En tercer lugar, analizaré las diversas constelaciones de casos que pueden producirse entre el delito de daños y el espionaje empresarial y sus posibles soluciones jurídico-penales, que deben partir en todo caso de un acceso o apoderamiento del objeto de los secretos empresariales como presupuesto previo, ya que de lo contrario no plantearía dudas con el espionaje[3]. Estos últimos

dichos elementos en los recursos que lo integran.

[2] De hecho, el bien jurídico del delito de daños ha sido identificado por la doctrina con la propiedad de la cosa, pero referida a la preservación de su integridad, incolumidad e incluso su existencia, así HERRERA MORENO, «Lección 8ª. Daños», en POLAINO NAVARRETE, (dir.), *Lecciones de Derecho penal. Parte especial*, 2011, p. 133.

[3] Así, no cabría duda de que existe solo un delito de daños si lo que se produce es un supuesto en el que un empresario, conocedor de los buenos resultados de su competidor, decide quemarle su oficina, a la que no entra para ello, o contrata un pirata informático o *hacker* para que le envíe un virus exclusivamente destructivo, que elimine toda su información, sin acceso a aquella.

casos llevarán a una solución u otra, dependiendo en gran medida de la finalidad que guíe la conducta de apoderamiento o acceso, para delimitar unos de otros, por lo que el elemento subjetivo del injusto va a jugar aquí un papel crucial.

2. *El delito de espionaje empresarial*

El Código penal de 1995 trajo consigo la tipificación del delito de espionaje empresarial, recogido en su artículo 278.1 CP, castigando con una pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses al "que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197". Este delito es susceptible de ser cometido por todo aquel que se hiciere con información empresarial ajena de carácter confidencial, a diferencia de lo que establecía el anterior artículo 499 del CP de 1973, que pasó a constituir el párrafo segundo del actual artículo 278 CP, como un tipo agravado de este, al establecer 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".

2.1. El bien jurídico protegido

Si bien el delito de espionaje fue una novedad del legislador penal de 1995, la revelación de secretos de empresa tiene su origen en nuestro ordenamiento jurídico en el CP de 1822, por lo que la doctrina viene pronunciándose desde antiguo acerca del bien jurídico protegido en el presente delito. Este fue cifrado en un primer momento en la intimidad, la propiedad o la libre voluntad del empresario, para después ser identificado por la doctrina más reciente con la leal competencia, la capacidad competitiva de la empresa o el interés económico del empresario en mantener la reserva[4].

Sin embargo, a mi juicio, el bien jurídico protegido en el presente delito lo constituye la propiedad de bienes inmateriales[5], los secretos empresariales, cuyo contenido se estudiará en el

[4] Defensores de estas últimas concepciones son, respecto de la leal competencia, entre otros, FERNÁNDEZ SÁNCHEZ, *Protección penal del secreto de empresa*, 2000, p. 110; MARTÍNEZ-BUJÁN PÉREZ, *Delitos relativos al secreto de empresa*, 2010, p. 18; MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., p. 434; SERRANO GÓMEZ/SERRANO MAÍLLO, *Derecho penal. Parte especial*, 15ª ed., 2010, p. 510; SERRANO-PIEDECASAS/DEMETRIO CRESPO, *Cuestiones actuales de Derecho penal empresarial*, 2010, p. 312. En relación a la capacidad competitiva de la empresa, BAJO FERNÁNDEZ, *Derecho penal económico aplicado a la actividad empresarial*, 1978, pp. 287 s.; LÓPEZ GARRIDO/GARCÍA ARÁN, *El Código penal de 1995 y la voluntad del legislador. Comentario al texto y al debate parlamentario,* 1996, p. 142, entre otros; y con referencia al interés económico del empresario en mantener la reserva, CARRASCO ANDRINO, *La Protección Penal del Secreto de Empresa*, 1998, p. 143; GÓMEZ RIVERO, *Nociones fundamentales de Derecho penal. Parte especial*, 2010, p. 471; MORÓN LERMA, *El secreto de empresa. Protección penal y retos que plantea ante las nuevas tecnologías*, 2002, pp. 129 s., entre otros.

[5] La doctrina civilista ha admitido la posibilidad de hablar de dominio sobre bienes inmateriales por vía de analogía, a través de la regulación legal de las llamadas "propiedades especiales", como son la propiedad industrial e intelectual, así DÍEZ-PICAZO/GULLÓN, *Sistema de Derecho Civil*, t. I, vol. III, Derechos reales en general, 8ª ed., 2015, p. 153. En el caso de los secretos de empresa existe un sistema más flexible en la relación que el titular tiene con la información que constituye secreto de empresa, dado el especial régimen por el que se rigen los secretos, según el cual, si alguien llega a conocer dicha información de forma lícita (por ingeniería inversa, por investigación independiente o por puro azar), no vulnera la citada relación, por no emplear medios ilícitos para

siguiente epígrafe. Lo que define a este tipo de propiedad es la facultad de aprovechamiento en exclusiva que tiene el titular del bien, como ocurre con los derechos de propiedad industrial y a diferencia de lo que sucede con la propiedad de bienes materiales.

Por un lado, los secretos constituyen el resultado de una actividad inventiva, intelectual o productiva, dando lugar todos ellos al capital intelectual de una empresa[6]. Las creaciones intelectuales que se encuentran en la base de los secretos de empresa tienen fundamento constitucional en el artículo 20.1.b) de la Carta Magna. Por otro lado, el ejercicio del derecho a la creación científica y técnica, contenido en dicho precepto, así como la libertad de empresa del artículo 38 CE, se materializan en la creación de empresas, cuya actividad deriva no solo en la propiedad de determinados bienes materiales, sino también, de esos otros inmateriales. Ambos tienen una naturaleza diversa, pero el carácter intangible de estos últimos no debe llevar a ubicarlos dentro de una esfera igualmente inmaterial o abstracta, pues también tienen un claro valor económico, equiparable en muchos casos al de ciertos bienes materiales, e incluso superior.

Sin embargo, hay que advertir que aquí se parte de una concepción funcional del patrimonio, de escasa acogida en la doctrina española[7], y según la cual, la propiedad no puede tener una protección absoluta por parte del Derecho penal, sino que este "ha de atender necesariamente a la *funcionalidad* que representa para su titular el objeto apoderado, apropiado o fraudulentamente obtenido", si se pretende seguir afirmando de este sector del Derecho su carácter fragmentario y subsidiario[8].

---

hacerse con ella. Ello es acorde con la concepción funcional de patrimonio de la que se parte, como veremos a continuación, pues, esta, a diferencia de lo que propugnaban las concepciones jurídicas, sobre todo, y la jurídico-económica, en menor medida, que definen el patrimonio dando especial protagonismo a la protección conferida por el ordenamiento jurídico, ciñe la idea de disponibilidad a situaciones fácticas de delimitación mucho menor, como señala GARCÍA ARÁN, *El delito de hurto*, 1998, p. 24. El patrimonio así entendido, permite concebir la propiedad en un sentido más laxo, aproximando los secretos de empresa a los derechos de propiedad industrial.

[6] En estos términos lo establece en su considerando (1), la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

[7] No ocurrió lo mismo en Alemania, donde esta concepción tuvo una amplia acogida, siendo precedida por la concepción personal de patrimonio que, como señala ZUGALDÍA ESPINAR, *Delitos contra la propiedad y el patrimonio*, 1988, p. 56, máximo exponente en nuestro país de esta última, lo identificaba con un derecho subjetivo al goce de los objetos, atendiendo exclusivamente a la voluntad individual como aspecto relevante de la propiedad, concepto del que tienden a desvincularse los autores alemanes, tal y como pone de manifiesto DE LA MATA BARRANCO, *Tutela penal de la propiedad y delitos de apropiación (El dinero como objeto material de los delitos de hurto y apropiación indebida)*, 1994, p. 80. La teoría personal ya avanzaba numerosos postulados que luego fueron acogidos por la teoría funcional. Los principales defensores de esta última en Alemania fueron, entre otros, OTTO, *Die Struktur des strafrechtlichen Vermögensschutzes*, 1970, pp. 63 ss.; BOCKELMANN, Paul, «Zum Begriff des Vermögensschadens beim Betrug», *JZ*, 1952, pp. 461 ss., quien afirmaba que esta teoría determina el alcance del patrimonio, así como la existencia y magnitud de los daños más bien atendiendo a las legítimas necesidades económicas y los intereses personales reconocidos al titular del patrimonio ("*Sie bestimmt den Umfang des Vermögens sowie Dasein und Ausmaβ des Schadens vielmehr nach dem berechtigen wirtschaftlichen Bedürfnis, dem anerkennenswerten persönlichen Interesse des Vermögensträgers*"). En España, junto a algún otro autor, los principales defensores de esta teoría son ASÚA BATARRITA, «El daño patrimonial en la estafa de prestaciones unilaterales (subvenciones, donaciones, gratificaciones). La teoría de la frustración del fin», *ADPCP*, 1993, pp. 123 ss.; DE LA MATA BARRANCO, *Tutela penal de la propiedad*, 1994, pp. 77 ss.; GALLEGO SOLER, *Responsabilidad penal y perjuicio patrimonial*, 2002, pp. 229 ss.

[8] DE LA MATA BARRANCO, *Tutela penal de la propiedad*, 1994, pp. 84 s. (cursiva añadida a la cita). Este autor pone de manifiesto que, puesto que nos encontramos en el ámbito de los bienes, esto es, de la relación de un sujeto con objetos concretos a los que reconoce una funcionalidad por su significado económico o por su capacidad para

Pues bien, para fijar la funcionalidad de los secretos de empresa hay que recordar que estos se ubican en el ámbito del Derecho de la competencia en sentido amplio, de igual forma a como ocurría con la propiedad industrial, estando su regulación civil en la Ley 3/1991, de 10 de enero, de Competencia Desleal. A partir de aquí se puede concluir que su *funcionalidad* radica en que estos elementos le permiten a su titular competir en el mercado para que su empresa consiga beneficios y evite pérdidas o impedir que otros adquieran una ventaja competitiva.

Partiendo de esta concepción, la estimación económica del secreto no puede medirse atendiendo exclusivamente al valor de mercado sino también, como afirma ASÚA BATARRITA, al "valor de uso", que se vincula principalmente a la finalidad de utilidad que cierto bien posee para su titular[9]. Si bien, como señala esta autora, el *criterio económico objetivo* opera como garantía de seguridad jurídica[10], el cálculo monetario que deriva de este deberá conjugarse, en la valoración del daño, con la *frustración de la utilidad pretendida*, no pudiendo tampoco ponderarse dicho daño atendiendo exclusivamente a esta última[11]. La interpretación de ASÚA BATARRITA constituye, como estima GARCÍA ARÁN, una reinterpretación del propio concepto de "valor económico", que no toma en cuenta exclusivamente el valor de mercado sino también el valor de uso que su titular pretende darle[12].

En definitiva, esta configuración del bien jurídico protegido en el delito de espionaje empresarial, que ha sido identificado con la propiedad de bienes inmateriales, es imprescindible para entender también el ataque a estos bienes en la configuración típica de otros delitos, como es el caso de los daños.

2.2. El concepto de secreto de empresa

Ya ha sido apuntado que el secreto de empresa constituye el elemento nuclear del espionaje empresarial, así como de otros tipos, como los previstos en los artículos 279 y 280 CP, que castigan respectivamente la revelación y utilización en provecho propio de secretos de empresa por quien tuviere legal o contractualmente el deber de guardar reserva, y dichos comportamientos cuando el sujeto activo de los mismos no ha participado en el descubrimiento del secreto empresarial, pero conoce su origen ilícito.

---

satisfacer intereses de su titular en conexión con su disfrute, es desde esta perspectiva desde la que hay que plantearse el sentido de la protección penal. De esta forma, -continúa diciendo el autor-, allí donde la injerencia de un tercero "suponga o pueda suponer una perturbación significativa de esas funciones, de esa potencialidad del titular en relación con los bienes que se encuentran en su ámbito de dominio y sean idóneos para satisfacer una necesidad individual, estaremos ante la realización del injusto de los delitos contra la propiedad" (p. 87).

[9] ASÚA BATARRITA, *ADPCP*, 1993, p. 104. A esta interpretación se adscribe, respecto al valor económico de la información como "valor de uso", MORÓN LERMA, *La tutela penal del secreto de empresa, desde una teoría general del bien jurídico*, 2002, pp. 58 s., quien afirma que dicho valor se singulariza "en virtud de las necesidades y preferencias de su poseedor, lo que determina que pueda diferir de un titular a otro", siendo el valor competitivo de la información "un valor relativo, referencial, que permite a su poseedor actuar estratégicamente y organizar su actividad económica del modo más rentable y beneficioso posible".

[10] ASÚA BATARRITA, *ADPCP*, 1993, p. 102.

[11] ASÚA BATARRITA, *ADPCP*, 1993, pp. 104, 107.

[12] GARCÍA ARÁN, *El delito de hurto*, 1998, p. 26.

El término extrajurídico de *secreto* se define en el Diccionario de la Real Academia de la Lengua Española como una "cosa que cuidadosamente se tiene reservada y oculta"[13]. Sin embargo, no existe en nuestro ordenamiento una definición legal de lo que constituye secreto[14], y tampoco secreto empresarial[15].

Por ello, para definir en sentido jurídico qué se entiende por secreto de empresa, es necesario acudir a los requisitos que establecen los textos internacionales. En primer lugar, la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas[16], cuyo artículo 2.1 prevé que se entenderá por tal la información que: a) sea secreta en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas; b) tenga un valor comercial por su carácter secreto[17]; c) haya sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control. En segundo lugar, hay que mencionar el Acuerdo de la Organización Mundial del Comercio sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), también conocido como *Acuerdo TRIPS*, por sus siglas en inglés —*Trade-Related Aspects of Intellectual Property Rights*—[18], cuyo artículo 39 de la Sección 7 prevé que, dentro de las esferas de propiedad intelectual que recoge el Acuerdo[19] se encuentra la información no divulgada, donde se incluyen los secretos comerciales y los datos de pruebas, definiéndolos con los mismos requisitos exigidos por la Directiva.

Los secretos de empresa, por tanto, pueden entenderse como una tipología de bien inmaterial, muy próximos a los derechos de propiedad industrial e intelectual, que pueden versar sobre información de diversa índole. En este sentido, GÓMEZ SEGADE puso de manifiesto que existían tres categorías de secretos de empresa: : i) los *secretos industriales*, que son aquellos "atinentes al sector técnico industrial de la empresa (procedimientos de fabricación, reparación o montaje, etc.)"[20]; ii) los *secretos comerciales*, concepto omnicomprensivo residual[21], constituido básicamente

[13] Primera acepción de la palabra "secreto" en el Diccionario de la RAE (Real Academia de Española), *online* en http://lema.rae.es (última visita: 27 de agosto de 2017).
[14] Véase GÓMEZ SEGADE, *El secreto industrial (Know-how). Concepto y Protección*, 1974, p. 64.
[15] Véase GALÁN CORONA, «Artículo 13. Violación de secretos», en BERCOVITZ RODRÍGUEZ-CANO, *Comentarios a la Ley de Competencia Desleal*, 2011, p. 354.
[16] Puede consultarse el texto completo de la Directiva en el siguiente enlace: http://www.boe.es/doue/2016/157/L00001-00018.pdf (última visita: 27 de agosto de 2017).
[17] Este valor comercial es en el que incide el llamado valor de uso, ya mencionado.
[18] Este es el Anexo 1C del Acuerdo de Marrakech por el que se establece la Organización Mundial del Comercio, firmado en Marrakech, Marruecos, el 15 de abril de 1994, cuyo texto puede consultarse en el siguiente enlace: https://www.wto.org/spanish/docs_s/legal_s/27-trips.pdf (última visita: 27 de agosto de 2017).
[19] Hay que tener presente, que el término en inglés *Intellectual property rights* comprende lo que en Derecho español se divide en dos categorías: "derechos de propiedad intelectual", esto es, los derechos de autor, y "derechos de propiedad industrial" (patentes, diseños industriales, modelos de utilidad, etc.).
[20] GÓMEZ SEGADE, *El secreto industrial*, 1974, p. 51. En el mismo sentido, BAJO FERNÁNDEZ/BACIGALUPO SAGGESE, *Derecho penal económico,* 2ª ed., 2010, p. 296; también TIEDEMANN, *Manual de Derecho Penal Económico. Parte Especial*, 2012, p. 232, quien afirma que "los secretos industriales se refieren a datos técnicos".
[21] MARTÍNEZ-BUJÁN PÉREZ, *Delitos relativos al secreto*, 2010, p. 28.

por información de carácter comercial[22], siendo la más relevante las listas de clientes, por ser objeto de la mayoría de casos que llegan a nuestros tribunales; y iii) los *secretos concernientes a otros aspectos de la organización interna* de la empresa y relacionadas con la misma[23].

La conducta típica principal del artículo 278.1 CP es el apoderamiento de secretos de empresa, cuyo sentido clásico debe abandonarse para comprender su ejecución en el presente delito[24]. Así, dada la especial naturaleza intangible de los secretos de empresa, dicho concepto no puede ser entendido en el sentido físico de la aprehensión de un objeto de carácter material, sino que debe interpretarse como una captación inmaterial de la información[25], que abarca todo tipo de conductas que, burlando las medidas de seguridad impuestas para proteger la información empresarial secreta, supongan la sustracción de esta del ámbito del titular sin su consentimiento y consiga ponerla bajo su dominio o control, pudiendo disponer de ella en cualquier momento.

2.3. La cláusula concursal del artículo 278.3 CP

El precepto que castiga el espionaje empresarial en el Código penal recoge en su apartado tercero una cláusula de cierre de carácter concursal, que establece que lo que aquel dispone "…se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos".

Fueron razones político-criminales, que primaban en las dos últimas décadas del siglo XX, las que dieron lugar a la inclusión de esta cláusula, dada la especial sensibilidad por la adaptación de la ley penal a la sociedad moderna, donde toda la actividad a nivel socioeconómico y, sobre todo, en el seno de la empresa, se realizaba ya a través de los medios informáticos[26].

Sin embargo, el carácter innecesario de esta cláusula es reconocido de forma unánime por la doctrina, bajo la crítica de que limitarla a los soportes informáticos no solo resulta inexplicable, sino además perturbador[27] y que nada aporta en relación con los criterios generales de resolución de concursos[28].

---

[22] CARRASCO ANDRINO, *La Protección Penal del Secreto*, 1998, p. 54.

[23] GÓMEZ SEGADE, *El secreto industrial*, 1974, pp. 51 s.

[24] En relación con los delitos relativos a la intimidad, ello ha llevado a la doctrina a plantearse hasta qué grado puede admitirse una espiritualización del concepto de apoderamiento sin que lleve consigo un desvío no permitido del principio de legalidad de los delitos, así ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, 2004, p. 84.

[25] Critican esta concepción amplia del apoderamiento en relación con los delitos relativos a la intimidad, ANARTE BORRALLO, «Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código Penal», *Jueces para la Democracia*, (43), 2002, p. 54; ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, p. 26.

[26] FERNÁNDEZ SÁNCHEZ, *Protección penal del secreto*, 2000, p. 286.

[27] Entre otros, ANARTE BORRALLO, «Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información», *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, (1), 2001, p. 245; BAJO FERNÁNDEZ/BACIGALUPO SAGGESE, *Derecho penal económico,* 2ª ed., 2010, p. 533; DOVAL PAÍS, «La intimidad y los secretos de empresa como objetos de ataque por medios informáticos», *Cuadernos del Instituto Vasco de Criminología*, (22), 2008, p. 114; FARALDO CABANA, *Las Nuevas Tecnologías en los Delitos contra el Patrimonio y el Orden Socioeconómico*, 2009, pp. 248 s.; FERNÁNDEZ SÁNCHEZ, *Protección penal del secreto*, 2000, p. 286; GONZÁLEZ RUS, «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», *Revista Electrónica de Derecho Penal y Criminología*, 01-14, 1999, II.2.A, quien califica esta cláusula de sorprendente; MARTÍNEZ-BUJÁN PÉREZ, *Delitos relativos al secreto*, 2010, p. 68;

Por un lado, como afirma, con razón, DOVAL PAÍS, la débil función preventivo-general o de otro tipo que pueden cumplir este tipo de previsiones, que no contribuyen a la economía legislativa y que no son extrañas en algunos tipos penales, se produce siempre a riesgo de comportar algún coste que - como afirma el autor, con gran parte de la doctrina -, viene constituido por la duda que plantea su falta de referencia a que dichas conductas recaigan sobre soportes no informáticos de los secretos[29]. Otra deficiencia de dicha cláusula, señalada también por la doctrina, radica en no aludir a los supuestos en que la conducta de destrucción recaiga sobre los datos contenidos en los soportes, esto es, en los elementos lógicos de estos y no así en los físicos, pues la conducta de apoderamiento sí viene recogida expresamente en el artículo 278.1 CP[30]. De estas dos ausencias precisamente se deriva la problemática a la que se aludirá seguidamente respecto al delito de daños.

No obstante, a mi juicio, a pesar de la presencia de una cláusula concursal no cabe duda de que tanto los supuestos expresamente mencionados por el legislador, como aquellos que ha omitido, reciben una respuesta penal en otros preceptos del Código y, por tanto, pueden dar lugar a concursos[31].

Por todas las razones expuestas parece que sería adecuada la supresión de esta cláusula concursal de *lege ferenda*. Esta genera una de sus peores consecuencias en la ausencia de mención expresa a la destrucción de los datos, frente a la inclusión de otros objetos, como son los soportes informáticos. Por ello, se hace necesario profundizar sobre todo en los supuestos de daños, que son los que mayores dudas plantean en relación con el espionaje empresarial.

MORALES PRATS/MORÓN LERMA, «Artículo 278», en QUINTERO OLIVARES (dir.)/MORALES PRATS (coord.), *Comentarios a la Parte Especial del Derecho Penal*, 10ª ed., 2016, p. 857.

[28] PRATS, «Descubrimiento y revelación de secretos de empresa en el Código penal de 1995», en DEL ROSAL BLASCO, *Delitos relativos a la Propiedad Industrial, al Mercado y a los Consumidores*, 1997, p. 193.

[29] En este sentido, DOVAL PAÍS, *Eguzkilore*, 2008, p. 114; FARALDO CABANA, *Las Nuevas Tecnologías*, 2009, pp. 248 s.; FERNÁNDEZ SÁNCHEZ, *Protección penal del secreto*, 2000, p. 286, quien afirma que en tanto que el legislador ha observado esta situación excepcional respecto de los soportes informáticos, no podrá producirse un concurso real en los supuestos en los que el apoderamiento sea de un soporte material distinto; GONZÁLEZ RUS, *REDPC*, 1999, II.2.A, quien señala que dicha cláusula dice literalmente que no se apreciará concurso de delitos cuando se trate, por ejemplo, de papeles, documentos escritos o medios audiovisuales; MARTÍNEZ-BUJÁN PÉREZ, *Delitos relativos al secreto*, 2010, p. 68, quien apunta que interpretando esta cláusula en su pura literalidad, dicha referencia imposibilitaría apreciar el concurso de delitos cuando la acción recaiga sobre otros soportes como, por ejemplo, cintas de vídeo que contengan información sobre un proceso productivo; MORALES PRATS/MORÓN LERMA, *Comentarios a la Parte Especial del Derecho penal,* 10ª ed., 2016, p. 857.

[30] Véase FARALDO CABANA, *Las Nuevas Tecnologías*, 2009, pp. 248 s.; FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 221; GONZÁLEZ RUS, *REDPC*, 1999, II.2.A, quien señala como ejemplos, el borrado del fichero o la eliminación de los datos en memoria volátil.

[31] De la misma opinión, FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 221; GONZÁLEZ RUS, *REDPC*, 1999, II.2.A; SANTANA VEGA, «Sección 3ª. De los delitos relativos al mercado y a los consumidores», en CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal,* p. 978, quienes estiman que entre los delitos que prevé la cláusula del párrafo tercero y los delitos del artículo 278.1 y 2 CP se da un concurso ideal (medial) de delito. En el mismo sentido, pero considerando que estamos ante bienes jurídicos distintos en los delitos del artículo 278 CP y los de apoderamiento o daños informáticos, careciendo de dificultad, por ello, la aplicación de las reglas concursales genéricas, MORALES PRATS/MORÓN LERMA, *Comentarios a la Parte Especial del Derecho penal,* 10ª ed., 2016, p. 857.

3. *El delito de daños*

Antes de aludir a los distintos tipos delictivos relativos a los daños hay que aclarar cómo se entienden estos, teniendo en cuenta que no existe un concepto legal al respecto[32]. Así, por daños en sentido penal puede entenderse toda destrucción o menoscabo de una cosa[33], incluyendo también su inutilización o deterioro. Dicho concepto es independiente del perjuicio patrimonial que el daño pueda ocasionar[34], que solo tendrá relevancia para determinar la responsabilidad civil derivada del delito[35], como ocurre también en el delito de espionaje empresarial.

De esta forma, se parte aquí de un concepto amplio de daños que debe atender también a la utilidad que el bien tiene para su titular, de acuerdo con la concepción funcional de patrimonio por la que se ha optado, y que tiene importantes implicaciones relacionadas con el secreto de empresa en los daños genéricos, pero sobre todo en los delitos de daños informáticos.

3.1. Los daños genéricos

El artículo 263 CP establece en su párrafo primero un tipo básico de daños en propiedad ajena, que no estén comprendidos en otros títulos del Código penal[36], y que prevé distinta penalidad en función de la cuantía del daño. Así, si esta excede de 400 euros se contempla una pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño; mientras que si es inferior a dicha cantidad, la pena de multa a imponer será de uno a tres meses, sustituyendo así a la anterior falta de daños del artículo 625 CP, que establecía una pena de localización permanente de dos a doce días o multa de diez a veinte días[37]. Junto a este primer apartado, el párrafo segundo recoge un tipo agravado de dicho delito en determinados supuestos, en los que no cabe ahondar en estos momentos.

Pues bien, son dos las cuestiones a destacar en este tipo delictivo que plantean problemas a los efectos que aquí interesan. En primer lugar, la naturaleza corporal del objeto material del delito,

[32] Véase CORCOY BIDASOLO, «Capítulo IX. De los daños», en CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código penal,* 2015, p. 926.
[33] Así MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, p. 409.
[34] Así MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, p. 409; ROBLES PLANAS/PASTOR MUÑOZ, «Tema 12. Delitos contra el patrimonio (III)», en SILVA SÁNCHEZ (dir.), *Lecciones de Derecho penal. Parte especial*, 2015, p. 293.
[35] Así CORCOY BIDASOLO, *Comentarios al Código Penal,* 2015, p. 928; FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 100; MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, pp. 409 s., quien afirma que con dicho entendimiento puramente descriptivo del daño patrimonial podría existir un delito de daño aunque este produzca un enriquecimiento del titular de la cosa dañada.
[36] De ahí que la doctrina lo considere un tipo residual frente a los específicamente tipificados en otros lugares del Código. Así, entre otros, CORCOY BIDASOLO, *Comentarios al Código Penal,* 2015, p. 927; HERRERA MORENO, *Lecciones de Derecho Penal,* 2011, p. 135.
[37] CASTRO CORREDOIRA/VÁZQUEZ-PORTOMEÑE SEIJAS, «La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP», en GONZÁLEZ CUSSAC (dir.), *Comentarios a la reforma del Código penal de 2015*, 2ª ed., 2015, p. 829, afirman que el cambio de falta a delito trasciende a lo meramente nominal, comportando un endurecimiento de la respuesta punitiva.

que puede ser una cosa mueble o inmueble[38]. Y, en segundo lugar, el carácter económicamente valorable de dicha cosa[39].

Resulta claro que la información empresarial de carácter reservado se contiene en objetos corporales como, por ejemplo carpetas, archivadores, cuadernos, libros u objetos que la contengan[40]. Respecto a los discos duros externos, equipos informáticos o parte de ellos, de acuerdo con DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, la destrucción o menoscabo de estos objetos quedarían subsumidos exclusivamente en el delito de daños genéricos, siempre que no se afecte a los datos o programas contenidos en el sistema ni a su accesibilidad (por ejemplo, la destrucción de un altavoz, del micrófono o del ratón), pues de lo contrario cabría hablar también de un delito de daños informáticos[41], bien en relación a datos o programas informáticos o documentos electrónicos (artículo 264 CP)[42] o al funcionamiento de sistemas informáticos (artículo 264 bis CP).

De esta forma, todo secreto de empresa contenido en soportes no informáticos es susceptible de ser destruido y su castigo iría solo por la vía del artículo 263 CP, en la medida en que no se trata de datos informáticos. Sin embargo, el problema que plantean estos supuestos es que, dado que el objeto sobre el que recae la conducta es una cosa material, el valor económico al que hace alusión el tipo iría en principio referido a esta, no considerándose en dicha cuantificación el de la información que contiene. Pongamos por caso que un empresario, temiendo los cada vez más sofisticados y frecuentes ataques a las telecomunicaciones, decide guardar una valiosa fórmula o información muy concreta en varias copias contenidas en diversas carpetas que a su vez guarda en distintas cajas fuerte. Si alguien se apodera de todas las carpetas y las destruye, atender exclusivamente al valor de los soportes no parecería una solución satisfactoria.

Teniendo en cuenta estos casos que, si bien poco frecuentes, podrían darse en la práctica, así como la concepción funcional de patrimonio de la que partimos en sede de bien jurídico, que deriva en un valor de uso del secreto que atiende a su utilidad o funcionalidad para una empresa concreta, hay que concluir que, en estos supuestos habrá que tener en cuenta el valor de la

---

[38] Véase GÓMEZ INIESTA, «Artículo 263», en ZAPATERO *et al.* (dirs.), *Comentarios al Código penal*, 2007, p. 591; HERRERA MORENO, *Lecciones de Derecho penal,* 2011, p. 135; MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, p. 411.

[39] Véase HERRERA MORENO, *Lecciones de Derecho penal,* 2011, p. 135; ROBLES PLANAS / PASTOR MUÑOZ, *Lecciones de Derecho penal. Parte especial*, 2015, p. 293.

[40] Un ejemplo de objetos que incorporan la información constitutiva de secreto de empresa se da en las SAP Barcelona, 8ª, 4.11.2002 (ARP\2003\221; MP: Jesús María Barrientos Pacho) y SJP León, 1ª, 9.2.2004 (ARP\2006\662; MP: Ignacio Javier Ráfols Pérez), en las que los códigos desencriptadores que eran objeto de aquel se encontraban en unas tarjetas que permitían emitir imágenes televisivas.

[41] En este sentido, DE LA MATA BARRANCO/HERNÁNDEZ DÍAZ, «El delito de daños informáticos: una tipificación defectuosa», *Estudios Penales y Criminológicos*, 2009, pp. 318 s.; 339 s., quienes afirman que la subsunción del ataque al *hardware,* que se refiere a todos los componentes físicos del sistema informático, no plantea mayores problemas de tipificación, pudiendo subsumirse en la modalidad del artículo 263 CP cuando la de los daños informáticos resultaba defectuosa; HERRERA MORENO, *Lecciones de Derecho penal,* 2011, p. 139, quien afirma que en los casos en que se produjeran daños físicos en el *hardware*, se daría un concurso medial de delitos entre los daños genéricos del artículo 263 CP y el de daños informáticos.

[42] La modalidad típica prevista en el artículo 264.1 CP, en virtud de la cual es considerado sabotaje informático dañar o deteriorar, por cualquier medio, datos o programas informáticos o documentos electrónicos, ampara la inclusión de estos supuestos en dicho tipo.

información contenida en el soporte material[43]. Lo contrario llevaría a soluciones absurdas y a una tutela insuficiente de la información si no se encuentra en documentos o soportes electrónicos, dando siempre lugar a la aplicación del delito leve y, por tanto, a una pena de multa de uno a tres meses, al no tener el soporte un valor que exceda de 400 euros[44]. Sin embargo, la exigencia de una cuantía económica que delimite los supuestos más graves del resto plantea un problema añadido que radica, no solo en la dificultad de evaluar económicamente un secreto de empresa, sino también en la poca importancia que se da a dicha tarea por parte de los empresarios[45].

Por último, difícilmente imaginables son los supuestos de alteración de la información en estos casos, que den lugar a la inutilización del secreto sin ser perceptibles por su titular. Sin embargo, también se estima que dichos casos pueden castigarse por la vía del artículo 263 CP, los cuales, generalmente, no irán más allá del delito leve.

3.2. Los daños informáticos o sabotaje informático

Cada vez son más los riesgos que presentan las nuevas tecnologías para la seguridad de la información. De ahí que la adopción de medidas por parte de los Estados miembros de la Unión para prevenir y reprimir conductas que atenten contra ella, constituya una cuestión de primer orden en el ámbito internacional. Por este motivo, el delito de daños informáticos ha sufrido numerosas modificaciones desde 1995, pretendiendo con ello dar respuesta a obligaciones de

[43] De la misma opinión, en relación a los menoscabos que podían sufrir los elementos lógicos del sistema mediante ataques al *hardware* cuando la tipificación de los daños informáticos era deficiente, DE LA MATA BARRANCO/HERNÁNDEZ DÍAZ, *EPC*, 2009, pp. 319 s. Así, estos autores afirmaban que esta interpretación suponía la asunción de un concepto funcional de propiedad, que atiende más que a la incolumidad de la sustancia de una cosa a la de su valor de uso real; MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, p. 410, estima al respecto que resulta excesivo calificar automáticamente de *daño* de una cosa toda alteración de su valor de uso, pero que, respecto a determinados objetos, en los que la inutilización de su posibilidad de uso equivale al daño de este, sí cabría hablar de daño del objeto, como ocurre, por ejemplo, al hacer inaccesible la utilización de un programa de ordenador. Así, el autor estima que en el caso del sabotaje informático en el concepto de daños sí se incluye la afectación de la posibilidad de uso de los datos, programas informáticos o documentos electrónicos, pues aquí el imposibilitar el uso del objeto material equivale al daño de de este mismo, debiendo hablar mejor de "sabotaje" (p. 414); ROBLES PLANAS/PASTOR MUÑOZ, *Lecciones Derecho penal. Parte Especial*, 2015, p. 293, quienes reconocen que, aunque discutido en la doctrina, es necesario tener en cuenta el valor de uso de la cosa, y no solo la lesión de su sustancia. En el mismo sentido, pero sin desatender a la afectación de la sustancia, que determine un menoscabo de la cosa que tenga incidencia en su propia existencia, suponiendo una pérdida de su valor real, independiente de los perjuicios derivados de la imposibilidad de uso, GONZÁLEZ RUS, *REDPC*, 1999, II.1.

[44] Muestra de ello es, por ejemplo, la solución a la que se llegó en la SAP Madrid, 5ª, 23.10.2015 (JUR\2015\274182; MP: Jesús María Hernández Moreno), en relación con el delito de apropiación indebida. En este supuesto se negó la concurrencia del delito por la inhabilidad de la información contenida en un disco duro para ser objeto de aquel pues, aun cuando la información pudiera ser susceptible de su consideración como activo patrimonial, su expresa referencia en dicho tipo había sido suprimida en la reforma de 2015, por lo que solo se condenó al sujeto por una falta de apropiación indebida del artículo 624.4 CP en redacción anterior a la entrada en vigor de la LO 1/2015, de 30 de marzo, por tener en cuenta el valor del disco duro retenido por el acusado, inferior a 400 euros.

[45] FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 101, apunta en este sentido que se derivan dos problemas de la peculiar naturaleza del objeto material en la determinación del valor del daño o resultado producido. Por un lado, la gran dosis de indeterminación respecto al valor de los datos en un ámbito de tan escasa tangibilidad. Y, por otro lado, que dicha prueba depende con frecuencia en exceso de la información que debe suministrar el titular de la información dañada. Ambos factores, afirma el autor, llevan a que el juez deba operar con criterios restrictivos de prudencia valorativa. Por su parte, FARALDO CABANA, *Las Nuevas Tecnologías*, 2009, p. 234, afirma que el titular de la información no siempre adopta medidas para protegerla porque no siempre es consciente de su relevancia.

ámbito europeo que han ido sucediéndose, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001, la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información o la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo. Sin embargo, los cambios en este ámbito no finalizan con estos textos, como ha demostrado la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, siendo este un asunto en constante cambio, que precisa la adaptación de la normativa en cuestión.

La idoneidad acerca de la ubicación sistemática entre los daños de estos delitos ha sido cuestionada por la doctrina, que defiende la necesidad de que se sitúen en un capítulo o sección independiente[46]. En cualquier caso, a los efectos que aquí interesan, partiré de la regulación de *lege lata*, sin entrar a valorar dicha cuestión y aludiré a los dos los tipos de daños que deben ser destacados en esta sede y que atentan contra datos o programas informáticos o documentos electrónicos, por un lado, y contra el funcionamiento de sistemas informáticos, por otro.

a) Daños o sabotaje de datos informáticos

El artículo 264.1 CP establece un tipo básico de daños informáticos cuyo objeto son los datos o programas informáticos o los documentos electrónicos ajenos, que se aplica cuando el resultado producido sea grave. La conducta en este tipo consiste en borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles los citados elementos, ello sin autorización, por cualquier medio y de manera grave, siendo la pena prevista la prisión de seis meses a tres años. Con esta tipificación, introducida con la LO 5/2010, de 22 de junio y modificada por la LO 1/2015, de 30 de marzo, se despeja a mi juicio la duda que cernía sobre este tipo de daños antes del año 2010, e incluso después, a pesar de la nueva redacción, que lo consideraba como un tipo agravado del previsto en el artículo 263 CP[47]. Junto a este párrafo primero, el segundo prevé un tipo agravado en determinadas circunstancias, entre las que cabe destacar aquí la de especial gravedad o afección a un número elevado de sistemas informáticos (apartado 2º) o el que se cometa utilizando los medios del artículo 264 ter CP (apartado 5º), novedad esta última de la reforma de 2015 y que castiga una serie de conductas que constituyen actos preparatorios de un delito

[46] Así, entre otros, ANDRÉS DOMÍNGUEZ, «XXXI. Reformas en daños», en QUINTERO OLIVARES (dir.), *Comentario a la reforma penal de 2015*, 2015, p. 549; DE LA MATA BARRANCO/HERNÁNDEZ DÍAZ, *EPC*, 2009, p. 321; MORÓN LERMA, *La tutela penal del secreto*, 2002, p. 609.

[47] De la misma opinión, CORCOY BIDASOLO, *Comentarios al Código Penal,* 2015, p. 932; MORÓN LERMA, *La tutela penal del secreto*, 2002, pp. 605 y 609, quien afirma que no debiera serlo en realidad pues constituye una figura autónoma con caracteres propios, pero que su inclusión en dicho capítulo lleva a esa conclusión. Esta consideración a mi juicio es equivocada, pues en cualquier caso estamos ante un tipo de daños, sin que ello suponga que estamos ante un subtipo agravado del previsto en el artículo 263 CP, ubicándose por ello en un precepto distinto. Asimismo, PICOTTI, «La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale», *Diritto penale e processo*, (6), 2008, p. 712, ha señalado que los datos, la información y los programas pueden hacerse inservibles con intervenciones como la alteración y la manipulación solo del *software*, sin afectar a la integridad del *hardware*. Ya lo pondría de manifiesto también dicho autor en uno de sus primeros trabajos sobre este tema, así PICOTTI, Lorenzo, «La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati», *Dir. Inf.*, 1986, p. 969.

informático[48]. Asimismo, el párrafo tercero del artículo 264 CP recoge una agravación de la pena cuando los hechos se hubieren cometido mediante la utilización ilícita de datos personales de otro para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Pues bien, en el tipo del artículo 264.1 CP se incluiría todo ataque a los datos informáticos, que constituye un supuesto frecuente en la actualidad. Aquí, el elemento típico que plantea una mayor problemática es la exigencia de que el resultado producido fuera grave[49], pues el legislador no ha establecido a qué ha de atender dicha valoración, existiendo tres posturas doctrinales al respecto. En primer lugar, según un grupo de autores, una interpretación sistemática obliga a atender al requisito previsto en el artículo 263 CP relativo a que la cuantía del daño exceda de 400 euros para determinar la gravedad del resultado[50]. En segundo lugar, otro sector doctrinal estima que no es indispensable atender a dicha cuantía, más aún cuando resulta complicado valorar monetariamente el perjuicio que causa la destrucción, alteración o inutilización de los datos[51]. Y, por último, hay quien defiende también que debe referirse al valor patrimonial del objeto material dañado o saboteado, sin aludir a una cuantía concreta, pero excluyendo daños morales, espirituales o intelectuales, aun cuando pudieran estos evaluarse en términos económicos, pero que servirán a los efectos de distinguir el daño patrimonial y el perjuicio patrimonial que ello cause[52].

En mi opinión, la exigencia de que supere los 400 euros no debe ser aplicada necesariamente a los daños informáticos. Partiendo del valor de uso como interés objetivo del secreto y de un concepto funcional de patrimonio, la gravedad nunca vendrá determinada por una cantidad estándar, la cual puede resultar grave en unos casos y no así en otros. Más bien habrá que atender al valor que tiene la información objeto de un secreto empresarial que ha sido borrada, dañada, deteriorada, alterada, suprimida o que se ha hecho inaccesible, en relación a una empresa, y en

48 En el mismo sentido se pronuncia MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, p. 416. Así, el artículo 264 ter CP establece literalmente: "Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:
a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

49 La doctrina critica la doble exigencia de gravedad que prevé este tipo al requerirla no solo respecto del resultado, sino también respecto de las conductas. Así CASTRO CORREDOIRA/VÁZQUEZ-PORTOMEÑE SEIJAS, *Comentarios a la reforma del Código penal*, 2ª ed., 2015, p. 831, considerándola redundante e innecesaria. Dicha exigencia, que viene impuesta por los textos internacionales, no se ha introducido, sin embargo, en otros ordenamientos, como es el caso del italiano, donde el legislador ha optado para acotar el tipo por dejar fuera ciertas conductas, en lugar de incluir esta cláusula. Hace esta crítica PICOTTI, *DPP,* 2008, p. 712.

50 Esta era la postura mantenida por CORCOY BIDASOLO/MIR PUIG, «Capítulo IX. De los daños», en CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal,* 2011, p. 590, quienes defendían una interpretación sistemática con el artículo 263. Sin embargo, la versión más reciente de esta obra suprime esta referencia sin añadir nada más (CORCOY BIDASOLO, *Comentarios al Código Penal,* 2015, p. 934). Así, en la línea de la opinión mantenida en este trabajo, parece que la tradicional postura doctrinal que abogaba por una dependencia de los daños informáticos respecto de los genéricos, tiende a desaparecer.

51 MORÓN LERMA, *La tutela penal del secreto*, 2002, p. 608.

52 MUÑOZ CONDE, *Derecho penal. Parte especial,* 20ª ed., 2015, pp. 414 s., quien estima que para valorar la gravedad del resultado deberá también considerarse la existencia o no de copias de seguridad de los datos, programas o documentos, o si la alteración producida, por ejemplo, mediante un virus, puede ser solucionada sin destruir o alterar dichos objetos.

términos de utilidad, lo cual no obsta a considerar el valor económico de aquella, pero también su valor funcional[53]. Así, será en el caso concreto cuando pueda definirse dicha gravedad, no constituyendo un delito de daños si no tiene dicho carácter.

No obstante, en la determinación de la gravedad del resultado y atendiendo al valor de uso o funcional, cabe plantearse el papel que juega la dificultosa recuperación del estado original de los datos o programas informáticos o documentos electrónicos, es decir, si estos se ven dañados con carácter definitivo o no, así como si la inutilización u obstaculización de sistemas informáticos tuviera dicho carácter. Pues bien, a mi juicio, no parece discutible que, si de esas acciones se derivara un efecto sobre los citados objetos que hace irrecuperable el estado original de estos en su integridad y disponibilidad, estaríamos ante un delito de daños informáticos, dada la gravedad del resultado producido. Ahora bien, todavía queda pendiente el interrogante de si quedarían fuera de estos tipos aquellos supuestos en los que dichos objetos fueran recuperables.

Esta cuestión tiene sentido en el presente juego entre el delito de daños y el de espionaje por la naturaleza inmaterial y el carácter ubicuo del objeto de estos, a diferencia de lo que ocurre en los daños genéricos, donde la destrucción de la cosa tiene un carácter irreversible, a menos que se trate de un bien fungible. En este sentido, cabría decir que aquellos supuestos en los que el estado original de los datos o programas informáticos o documentos electrónicos, así como el normal y correcto funcionamiento de los sistemas informáticos, fuera recuperable, esto es, no tuviera carácter definitivo, también cabría hablar de un delito de daños informáticos, siempre que ello tuviera lugar de forma duradera o por el tiempo suficiente para generar una perturbación sustancial en la utilidad que dichos objetos reportan[54]. En esta valoración habrá que tener en cuenta, entre otros aspectos, los costes de recuperación de la información suprimida o alterada[55], la relevancia que esta posee para la actividad empresarial (tanto si juega un papel importante como si se trata de información de un valor tan irrisorio que pudo seguir funcionando como siempre, prescindiendo absolutamente de ella), si la inutilización se produjo por un periodo de tiempo en el que la empresa estaba cerrada (por ejemplo, domingos o festivos), etc. Todo ello deberá tenerse en cuenta, independientemente de la cuantía a la que finalmente ascienda la responsabilidad civil.

---

[53] La consideración del valor funcional junto al económico, salva la crítica que vierte un sector de la doctrina, como FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 100, quien afirma que el criterio del valor funcional aproxima demasiado el concepto de daño al de perjuicio, o GONZÁLEZ RUS, *REDPC*, 1999, II.1, que critica la solución de apelar exclusivamente al valor de uso para determinar si concurre el delito o no, en la medida en que ello – advierte -, "supone confundir el daño a la cosa con el perjuicio, cuya presencia no resulta determinante para la configuración del delito".

[54] DE LA MATA BARRANCO/HERNÁNDEZ DÍAZ, *EPC*, 2009, p. 320, estiman también que la imposibilidad de utilización a la que puede dar lugar un delito de daños, puede ser tanto definitiva como temporal. Así también, respecto del delito de apropiación indebida en relación con la expropiación, que constituye la privación al sujeto pasivo de las facultades que se derivan de su condición de propietario, DE LA MATA BARRANCO, *Tutela penal de la propiedad*, 1994, p. 148. También considera que la inutilización puede ser parcial o total, temporal o definitiva, FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 93.

[55] En el mismo sentido, FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 100, quien señala que "los datos afectados por los ataques que tienen lugar en el ámbito de Internet son, con frecuencia, elementos que no están en el mercado (v. gr. lista de clientes)", de ahí que defienda el recurso en este ámbito al criterio del coste de recuperación o restablecimiento de la información o del sistema.

En todo caso, la gravedad del resultado que exige el tipo del artículo 264.1 CP no podrá ser tal que dé lugar a la obstaculización o inutilización del funcionamiento del sistema informático, ya que ello formaría parte del delito previsto en el artículo 264 bis.1.a) CP.

Por último, hay que apuntar que la reforma de 2015 ha aumentado el límite máximo del marco penal previsto para este delito en un año, estableciendo así una pena de seis meses a tres años y equiparándola a la de daños en el funcionamiento de sistemas informáticos, cuya gravedad parece mayor, como hasta ahora estaba previsto.

b) Daños o sabotaje de sistemas informáticos

Por último, hay que aludir al artículo 264 bis CP, el cual establece el delito de sabotaje a sistemas informáticos castigando con la misma pena del precepto anterior al que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, lo cual puede tener lugar de alguna de las siguientes formas: a) realizando alguna de las conductas a las que se refiere el artículo 264 CP; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Este precepto, además, establece la aplicación de la pena en su mitad superior, pudiendo llegar hasta la superior en grado, cuando los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, de un negocio o de una Administración pública. Como ocurría respecto del carácter grave del resultado en el precepto anterior, aquí tampoco ha previsto el legislador indicación alguna sobre los criterios a tener en cuenta para apreciar la relevancia del perjuicio en la actividad empresarial[56], por lo que deberá determinarse en el caso concreto, atendiendo a los aspectos ya mencionados, entre otros.

4. La casuística posible entre daños y espionaje

4.1. Punto de partida: acceso previo y dimensión subjetiva compatible

Una vez vistas las cuestiones más relevantes para el objeto de estudio sobre la tipificación del espionaje empresarial y las características de los tipos de daños, así como las cuestiones problemáticas a las que se enfrentan, que repercuten en el secreto de empresa como objeto de la conducta, vamos a ver a continuación la posible casuística que puede darse entre ambos tipos delictivos como ataques al bien inmaterial de la información empresarial.

El punto de partida radica aquí en un acto de apoderamiento o acceso previo que debe tener lugar sobre el secreto de empresa como presupuesto necesario del delito de espionaje. Sin embargo, el hecho de que dicho acto haya tenido lugar, no significa que estemos ante este último delito. Para deslindar las constelaciones de casos que pueden producirse juega un papel crucial el elemento subjetivo del injusto del espionaje frente al dolo exigido en el delito de daños. La

[56] CASTRO CORREDOIRA/VÁZQUEZ-PORTOMEÑE SEIJAS, *Comentarios a la reforma del Código penal*, 2ª ed., 2015, p. 832, afirman que ello deja la puerta abierta al arbitrio judicial.

dimensión subjetiva cumple así una doble función: por un lado, una *restrictiva* que atiende al bien jurídico protegido; y, por otra, una *delimitadora* respecto de otras figuras afines, facilitando la resolución de problemas concursales, lo cual resulta clave en este contexto[57]. Por ello, dado que el Código penal protege la propiedad de un individuo de diversas maneras, habrá que atender a las formas de ataque a esta y a la intención del autor al llevarlas a cabo.

Así, la sustracción de un secreto de empresa con ánimo de desentrañar su contenido, descubriéndolo y quedándose con él para poder disponer de él en un futuro, o bien hacerlo para ponerlo en conocimiento de otro, dará lugar a la conducta de espionaje empresarial; mientras que dicha sustracción, cometida con la intención de acabar con la propiedad del titular sobre el secreto mediante su destrucción, inutilización o menoscabo deliberado, por el mero placer de perjudicarlo y sin perseguir utilidad alguna, constituirá un delito de daños[58]. De dicha destrucción puede resultar una posible ventaja competitiva si esta es cometida, por ejemplo, por un competidor que deja a su rival en la quiebra. Sin embargo, ello pertenecería ya al agotamiento del delito de daños, si dicha ventaja no parte de un aprovechamiento de dicha información[59]. Lo que ocurre aquí, y donde radica la especial problemática, es que ambas intenciones son compatibles en el presente caso, dado el carácter inmaterial del bien en que se encarna la propiedad. Dicho carácter hace que el espionaje, en general, o el apoderamiento de secretos de empresa, en particular, no impliquen siempre una desposesión y, por tanto, la pérdida definitiva de aquellos por parte de su titular. Así, será habitual que el secreto se sustraiga sin levantar sospechas y conviva bajo el dominio de ambos sujetos, activo y pasivo. Por ello, habrá que prestar especial atención a los supuestos en los que dicha desposesión pueda producirse,

[57] En el mismo sentido, GUTIÉRREZ FRANCÉS, «Delincuencia económica e informática en el nuevo código penal», *Cuadernos de derecho judicial*, 1996, p. 275, quien señala que las fronteras entre estas grandes categorías no son siempre nítidas, ya que la dinámica comisiva propicia situaciones concursales. Así -continúa diciendo el autor- "no será infrecuente que un comportamiento de espionaje empresarial vaya acompañado de una modificación o destrucción de datos, subsumible en la categoría de sabotaje informático; o que la intrusión subrepticia de un 'hacker' en un sistema de procesamiento automático de datos desemboque en una modificación o supresión de datos, de extraordinarias consecuencias económicas para la víctima, lo cual nos trasladaría desde el intrusismo informático a los terrenos del sabotaje (…). En consecuencia, será la dimensión subjetiva de la conducta la que, con frecuencia, nos aporte el criterio delimitador en cada caso"; MARTÍNEZ-BUJÁN PÉREZ, *Delitos relativos al secreto*, 2010, p. 56; MORALES PRATS, «Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en QUINTERO OLIVARES (dir.)/MORALES PRATS (coord.), *Comentarios a la Parte Especial del Derecho Penal*, 10ª ed., 2016, pp. 411 s.; MORÓN LERMA, *La tutela penal del secreto*, 2002, p. 853; PRATS, *Delitos relativos a la Propiedad Industrial,* 1997, p. 193.

[58] En este sentido también, CORCOY BIDASOLO, *Comentarios al Código penal,* 2015, p. 928. Un sector doctrinal, incluye, sin embargo, como posible intención del espionaje la destrucción del secreto. En este sentido se pronuncian, ESTRADA I CUADRAS, *Violaciones de secreto empresarial. Un estudio de los ilícitos mercantiles y penales*, 2016, p. 65; MORÓN LERMA, *El secreto de empresa*, 2002, p. 307, nota 27. A mi juicio, no parece adecuado incluir dicha finalidad en el elemento subjetivo del espionaje, pues como he mencionado, esta cumple una función delimitadora determinante para distinguir ambos delitos.

[59] La doctrina ha puesto de manifiesto que los delitos de daños constituyen infracciones contra el patrimonio cuyo rasgo común es que no se orientan a un enriquecimiento ilícito. En este sentido, FERNÁNDEZ TERUELO, *Derecho penal e internet,* 2011, p. 93; HERRERA MORENO, *Lecciones de Derecho penal,* 2011, p. 133, quien afirma que se trata de conductas eminentemente destructivas, aunque compatibles con diversas motivaciones criminales, ajenas a la tipicidad, que pueden integrarse en una fase de agotamiento no delictivo o que, en todo caso, pueden dar lugar a que concurran los elementos típicos de otro delito, lo que se produce en el tercer grupo de casos que a continuación veremos. En sentido similar, ROBLES PLANAS/PASTOR MUÑOZ, *Lecciones de Derecho penal. Parte Especial*, 2015, p. 292, quienes estiman que en los daños no tiene lugar una apropiación en sentido estricto, sino exclusivamente una expropiación de la cosa.

exponiéndose seguidamente las distintas constelaciones de casos que pueden tener lugar y las soluciones jurídico-penales a las que puede llegarse.

4.2. Supuestos que se agotan en un delito de daños

Para empezar hay que aludir a los casos que se agotan exclusivamente en un delito de daños cuando, de haber concurrido determinadas circunstancias, podrían haber dado lugar también a espionaje.

En primer lugar, en este grupo se encontrarían aquellos supuestos en los que un sujeto *se apodera del soporte donde se contiene la información, pero, en lugar de quedarse con ella, simplemente la destruye*. Esto ocurrió en el caso juzgado por la SAP Madrid, 6ª, 3.6.2013 (JUR\2013\207748; MP: Pedro Javier Rodríguez González-Palacios), en el que el empleado de un estudio de arquitectura se llevó un ordenador, devolviéndolo finalmente bloqueado para impedir el acceso a su titular, y habiendo borrado siete archivos de los que dos se perdieron definitivamente y cinco pudieron recuperarse gracias a las copias que su titular había hecho previamente. Aquí solo se aplicó un delito de daños al funcionamiento de sistemas informáticos por haberlos obstaculizado, sin constatarse que se apoderara de información alguna. La gravedad del resultado en este caso no resultó valorada, pronunciándose el tribunal solo en contra de la aplicabilidad a este delito del requisito del artículo 263 CP respecto al límite de 400 euros.

En segundo lugar, otro supuesto que se enmarcaría en este grupo es el caso en el que un sujeto *accede de forma ilegítima al sistema informático de una empresa mediante un determinado tipo de virus y, pudiendo realizar un copiado de toda o parte de su información para aprovecharse de ella, lo que hace es borrarla o alterarla exclusivamente*. Tal fue el caso en el que se pronunció la SAN (Sala de lo Penal, Sección 4ª) 17/2015, de 11 de junio, en el que los tres acusados fueron infectando ordenadores con un programa malicioso, creando así una red zombi (*botnet*) de estos, que los convertía en robots controlados remotamente por el sistema responsable (*bot-master*). Las finalidades de estas redes zombis pueden ser diversas y entre ellas se incluye la del apoderamiento de datos o documentos que constituyan secreto empresarial. Sin embargo, en este caso la finalidad con la que se creó fue la de realizar ataques de denegación de servicios en páginas webs, lo cual afectó a más de cien empresas. Por estas acciones se les impuso una pena de un año de prisión por un delito continuado de daños del actual artículo 264 bis CP, si bien en la actualidad este caso podría subsumirse en el apartado segundo de dicho tipo, aumentando considerablemente la pena por la concurrencia de la circunstancia agravante prevista en el artículo 264.2.2ª CP, al afectar a un número elevado de sistemas informáticos.

En ambos supuestos, aunque el sujeto que realiza la conducta de daños llegara a leer la información, si su finalidad es destruirla y no aprovecharse de ella, estaríamos exclusivamente ante un delito de daños.

Distinto sería el caso en que el responsable de dicha red, como apunta la propia sentencia como posibilidad de estos ataques, que se da con frecuencia, la alquilara a un tercero. En estas situaciones, aun cuando el sujeto a quien se la alquilara tuviera también intención de destruir la información o de producir una obstrucción de los sistemas, estaríamos ante un supuesto que

entraría en el tercer grupo de casos que veremos más adelante. Así, por un lado se daría el delito de daños del artículo 264 bis CP en los ataques de denegación de servicios y, por otro, la revelación de secretos de empresa ilegítimamente obtenidos del artículo 278.2 CP.

Los dos supuestos mencionados que constituirían delitos de daños informáticos, lindan con el espionaje por producirse un apoderamiento previo del soporte donde se contiene la información (primera hipótesis) o un acceso informático a esta (segunda hipótesis), pero en nada difieren estos casos en la práctica de aquellos en los que lo que se produce es la destrucción física del soporte o del local donde se encuentran estos, dando lugar a un daño en propiedad ajena como cuando el objeto del delito lo constituye, por ejemplo, maquinaria o material de producción de la empresa.

4.3. Supuestos que se agotan en un delito de espionaje

Un segundo grupo de supuestos son aquellos en los que solo se produce un delito de espionaje empresarial. Es evidente que tendrá lugar un delito de espionaje en aquellos supuestos, frecuentes por lo demás, en los que un sujeto se apodere de la información sin desposeer a su titular de ella o destruirla. Así ocurrió, por ejemplo, en la SAP Tarragona, 2ª, 4.4.2003 (JUR\2003\210233; MP: Xavier Nouvilas Puig), en la que se condenó al acusado por un delito de espionaje empresarial por acceder a diversos códigos fuente creados por la empresa y a una base de datos con información sobre cuentas de acceso a internet y correo electrónico de numerosos clientes, copiándolos e instalándolos en un ordenador personal de su domicilio, sin destruir información de la empresa.

Además de este tipo de supuestos, a mi juicio, constituyen exclusivamente espionaje empresarial los casos en los que un sujeto se apodera de soportes informáticos o documentos escritos donde se contiene la información confidencial, que copia, destruyendo dichos soportes y documentos posteriormente, sabiendo que existen más copias de estos (por ejemplo, si sustrae una fotocopia de otro original o un CD que se entrega a determinados empleados con información confidencial). Sin embargo, si se apodera de la única copia existente para aprovecharla, sacándola a su vez del ámbito de dominio de su titular, habrá que valorar si dicha conducta constituye un delito de daños, excediendo así el desvalor del espionaje empresarial o si, por el contrario, entra dentro de este.

Pues bien, en estos casos generalmente el sujeto no tiene por qué saber que se apodera de la única copia existente, en la medida en que, tratándose la información de un bien de carácter inmaterial, lo más lógico será que el titular haya sido diligente y realizado copias. Además, no cabe esperar que el sujeto que ha cometido dicha conducta devuelva el soporte del que se apodera, siendo lo más probable que lo destruya para eliminar pruebas. En este sentido, a mi juicio, en la medida en que el apoderamiento de soportes informáticos y documentos escritos que prevé el tipo puede conllevar en ciertas ocasiones la desposesión al titular de sus secretos empresariales, aunque no sea necesario ni habitual, los casos en los que se apodera de la única copia existente deberán quedar comprendidos en el desvalor del tipo del artículo 278.1 CP. Esta conclusión parte del

principio de autoprotección del titular del secreto[60], que tiene que adoptar todas las medidas pertinentes para proteger su información, lo cual no parece producirse si de esta existe solo una única copia.

No obstante, aquellos supuestos en los que el sujeto sea plenamente consciente de que, por ejemplo, sustrayendo el portátil de su competidor para aprovecharse de su información confidencial, y destruyéndolo posteriormente de forma deliberada, acabará con todas las copias de la información que este tenía y que estaban almacenadas en él, podrá estimarse que se da un dolo directo de segundo grado o de consecuencias necesarias respecto al delito de daños del artículo 264 CP, resolviéndose este caso mediante un concurso de leyes por consunción a favor del delito de espionaje empresarial[61].

Por último, hay que advertir que cuando el atentado se produce respecto a todas las copias existentes, con el claro objetivo de aprovecharse de la información y sacarla de su ámbito de dominio o cuando tiene lugar el borrado, alteración o cualquier otro tipo de conducta sobre los datos informáticos, adicionalmente a su apoderamiento, podrán concurrir ambos delitos, entrando este supuesto en el tercer grupo de casos.

4.4. Supuestos en los que concurren espionaje y daños

Por último, podrán producirse diversos supuestos que darán lugar a concursos de delitos entre el espionaje empresarial y los distintos tipos de daños. En este tercer grupo se encuentran, sobre todo, aquellos casos en los que el acceso y el apoderamiento se producen sobre datos informatizados, siendo posible ver, de forma más clara respecto de los anteriores, la doble intencionalidad de descubrimiento y destrucción o menoscabo de aquellos.

Así, por un lado, puede darse el caso en el que un sujeto se apodere de un disco duro de la empresa competidora, copie la información en uno propio y la borre o le introduzca un virus que la haga inaccesible, dando lugar a que el titular ya no disponga de esta[62]; o bien cuando, al

---

[60] HÖRNLE, «Subsidiariedad como principio limitador. Autoprotección», en VON HIRSCH *et al.* (ed. alemana) y ROBLES PLANAS (ed. española), *Límites al Derecho penal. Principios operativos en la fundamentación del castigo*, 2012, p. 90. Esta autora apunta que, "del carácter de *ultima ratio* del Derecho penal no sólo tendría que derivarse la necesidad de, en su caso, dar preferencia a los medios de protección estatal más leves, sino también como ulterior consecuencia la renuncia a la pena cuando el afectado no hubiera usado los medios de autoprotección a los que sin más le era posible y exigible recurrir". En el mismo sentido, MIR PUIG, *Derecho penal. Parte general*, 9ª ed., 2011, p. 118.

[61] Un caso que merece comentario en este contexto, es el que juzgó la SAP Madrid, 5ª, 23.10.2015 (JUR\2015\274182). En este supuesto, aunque el delito que se cuestionaba junto al de daños informáticos era el de apropiación indebida de un disco duro externo donde se contenía información empresarial relevante, se estimó que la sustracción de aquel conllevaba la inutilización de los datos informáticos almacenados en él, al hacerlos inaccesibles y que quedaran fuera del alcance del legítimo dueño del sistema informático. El delito de daños informáticos finalmente no se aplicó por no considerarse el resultado producido como grave, al no darse detalle de la información concreta afectada y aludir a ella solo con carácter vago y genérico.

[62] La concurrencia de estos casos es relativamente frecuente. Así, un supuesto de esta índole tuvo lugar en el AAP Barcelona, 2ª, 18.7.2012 (JUR\2012\403963; MP: Jaume Rodes Ferrández), en el que la acusación solicitaba la condena de una empleada de su empresa por un delito de apropiación indebida de un ordenador de esta, un delito de apoderamiento de secretos de empresa del artículo 278.1 CP y otro de daños informáticos del artículo 264 CP. En el presente caso, la acusada se llevó el ordenador con numerosa información de la que se apoderó y, cuando lo devolvió, dos pruebas periciales informáticas demostraron que, además, había usado un programa llamado "Ccleaner", con el que borró el disco duro, sin posibilidad de recuperarlo, y desinstalando seguidamente

introducirse en el sistema informático ajeno, tras realizar el copiado de la información, decide alterarla, de forma que, en lugar de desposeer al titular de esta, hace que continúe usándola pero de modo perjudicial para su empresa, mientras que el que los sustrae se beneficia de ellos[63]. Todos estos supuestos serían daños de los previstos en el tipo del artículo 264 CP. Por otro lado, también puede tener lugar cuando la utilización de un programa malicioso obstaculiza o interrumpe el normal funcionamiento de un sistema mientras se produce el copiado masivo de la información contenida en él, dando así lugar al tipo del artículo 264 bis CP[64].

En estos casos, a mi juicio, podrán darse varias soluciones[65]. Así, en los supuestos en los que, a medida que se copia la información, se procede a su borrado o alteración, estaremos ante un concurso ideal de delitos, partiendo de la teoría de la unidad natural de acción[66]. Tal sería el caso,

---

dicho programa. Otro caso en el que, sin embargo, se condenó solo por un delito de espionaje empresarial del artículo 278.1 CP, tuvo lugar en la SAP Barcelona, 2ª, 9.3.2006 (JUR\2006\227208; MP: Javier Arzua Arrugaeta), en el que la acusada realizó una copia de los archivos relativos a ofertas para nuevos concursos públicos, de interés para la competencia, destruyendo la existente en la empresa. También ocurrió un supuesto similar en la SAP Sevilla, 7ª, 30.12.2011 (ARP\2012\305; MP: Esperanza Jiménez Mantecón), en la que los dos acusados se apoderaron de forma ilegítima de información comercial secreta de la empresa para la que trabajaban con la intención de fundar una propia, pero uno de ellos, además, realizó un borrado masivo de datos contables y fiscales, que además fue selectivo, respecto los de un determinado valor para la empresa, lo cual fue determinante para constatar que no fue un virus el que accidentalmente produjo dicha pérdida.

63 Piénsese en el caso en el que la alteración de una fórmula pueda dar lugar a la fabricación de un producto defectuoso o que la modificación de los datos contenidos en una lista de clientes, como pueden ser sus teléfonos, correos electrónicos, preferencias comerciales o la introducción de otros falsos, derive en pérdidas en las ventas de la empresa.

64 Un caso similar se juzgó por la SJP Terrassa, 1ª, 1.2.2006 (JUR\2006\113871; MP: Desconocido), en el que se produjo un apoderamiento de las claves de acceso a una página web mediante engaño a su proveedor, haciéndose pasar por su legítimo titular, para así, por un lado, bloquear su acceso al público e impedir su control comercial por este; y, por otro, cambiar el dominio de la página, llegando a negociar el espacio en internet con otro proveedor para su utilización por una empresa distinta. En este supuesto finalmente se condenó al acusado por un delito de descubrimiento de secretos de empresa del artículo 278.1 CP y, además, por una falta de daños del derogado artículo 625 CP, por considerarse que no quedaba demostrado que los daños ascendieran a 400 euros, haciéndose por tanto extensible a dicho tipo el requisito de los daños genéricos. Actualmente, este supuesto podría castigarse por la vía del artículo 264.3 CP, por haber utilizado de forma ilícita (mediante engaño), los datos personales de otra persona (el legítimo titular de la página), ganándose así la confianza del proveedor y facilitándose el acceso a los datos o programas informáticos.

65 La doctrina no es unánime respecto a las consecuencias jurídico-penales a las que dan lugar estos supuestos. Así, CASTRO MORENO, «El Derecho penal español ante el espionaje industrial y el secreto de empresa (artículos 278-280 CP)», *RTDPE,* (I-2), 2006, p. 51, afirma que en aquellos casos en los que mediante el mismo apoderamiento o interceptación de los secretos, se lesionen, a su vez, los intereses económicos mercantiles de la empresa, estaríamos ante un posible concurso de delitos, especialmente ideal; por su parte, FERNÁNDEZ SÁNCHEZ, *Protección penal del secreto*, 2000, p. 287, considera que en el supuesto de que junto a una de las conductas tipificadas en el art. 278.1 y 2 CP concurra un delito de destrucción de soportes informáticos, estamos ante un concurso real; por último, BAJO FERNÁNDEZ *et al.*, *Manual de Derecho Penal. Parte Especial. Delitos patrimoniales y económicos,* 2ª ed., 1993, p. 49, estiman que cuando un acto de disposición a título de dueño sobre la cosa consiste en su destrucción, este será un acto posterior copenado si es posterior a un delito de apoderamiento, defraudación o apropiación, mientras que, si dicha destrucción no sucede a ningún otro delito patrimonial, estaremos en presencia de un delito de daños. La primera alternativa de esta última postura responde, como señala MIR PUIG, *Derecho penal. Parte general*, 10ª ed., 2016, p. 686, a que los actos posteriores impunes o copenados "constituyen la forma de asegurar o realizar un beneficio obtenido o perseguido por un hecho anterior y no lesionan ningún bien jurídico distinto al vulnerado por ese hecho anterior ni aumentan el daño producido por el mismo".

66 En la teoría de la unidad natural de acción, como señala DÍEZ RIPOLLÉS, *Derecho Penal Español. Parte General*, 4ª ed., 2016, p. 567, la unidad de acción se consigue agrupando en una sola acción todos los movimientos corporales dirigidos sin solución de continuidad a la consecución de un mismo fin e interpretando dicha ausencia de solución de continuidad como la unión espacio-temporal entre dichos movimientos, de forma que dé lugar a que un observador imparcial los estime como unidad.

por ejemplo, si tras copiar la información para su descubrimiento y posible aprovechamiento posterior (acción que constituye un delito de espionaje), en lugar de apagar el ordenador, este se formatea. Sin embargo, en aquellos casos en los que, además de la reproducción de la información mediante cualquier vía, se instala posteriormente un programa que la destruye o la altera, se envía un troyano telemáticamente con la misma finalidad, así como los casos en los que se produce una obstaculización o interrupción del funcionamiento de sistema, estaremos generalmente ante un concurso real de delitos, en la medida en que pueden identificarse dos unidades de acción natural que se corresponden con varias unidades de acción típica.

Un supuesto de concurso real se daría también en el caso, mencionado previamente, en el que el sujeto responsable de causar daños a datos, programas o sistemas informáticos a través del empleo de códigos maliciosos que permiten un control remoto del ordenador así como de toda la información contenida en él, decidiera negociar con un tercero la transmisión de dicho acceso ilegítimo. En estos casos, frecuentes por lo demás, como señalaba la SAN (Sala de lo Penal, Sección 4ª) 17/2015, de 11 de junio, se daría dicho concurso entre el delito de daños en cuestión que tuviera lugar y el de revelación de secretos de empresa, mediante el artículo 278.2 CP. Este último precepto no exige elemento subjetivo alguno para su consumación, sino solo que se comunique a un tercero un secreto ilegítimamente obtenido, por lo que el tipo se daría en este supuesto.

5. Conclusiones

Una vez tratadas las cuestiones más relevantes sobre la regulación del delito de daños y del espionaje empresarial, en relación al objeto de estos cuando viene dado por un bien inmaterial como es la información, pueden extraerse las siguientes conclusiones.

En primer lugar, la propiedad inmaterial presenta diversas formas de ataque, al igual que la de carácter material. Sin embargo, la diferencia principal con los bienes objeto de esta última radica en la posibilidad de reproducir los de la primera, dando lugar a un posible disfrute de los mismos de forma simultánea por parte de su titular y del autor del ataque. Ello hace necesario que el Derecho penal responda atendiendo a dichas particularidades.

En segundo lugar, en el caso del espionaje empresarial, dada la especial naturaleza de la información, la conducta típica de apoderamiento debe entenderse asimismo en un sentido inmaterial para abarcar todos los supuestos que puedan producirse. Además, la cláusula concursal se estima innecesaria para la resolución de los problemas concursales, al no aludir a los supuestos en que se produzca el apoderamiento o la destrucción de los soportes no informáticos, ni a cuando esta última acción recaiga sobre los datos contenidos en los soportes. Por estos motivos, se consideraría adecuada su supresión de *lege ferenda*. No obstante, de *lege lata*, nada obsta para aplicar las reglas concursales genéricas tanto a los supuestos previstos en la cláusula, como a los que no lo están.

En tercer lugar, la concepción funcional de patrimonio de la que se parte permite responder de forma satisfactoria a los diversos problemas derivados de la especial naturaleza de los bienes

inmateriales, sobre todo en relación a los daños. Por un lado, en relación a la regulación de los daños genéricos del artículo 263 CP, la alusión al valor económico del objeto no puede ir referida solo al soporte material, sino también a su contenido, atendiendo no solo al valor de mercado sino también al de uso de la cosa, pues de lo contrario no se estaría protegiendo la información. Por otro lado, por lo que respecta a los daños informáticos del artículo 264 CP, y como consecuencia de la citada concepción, la exigencia de gravedad del resultado y de la conducta no puede venir condicionada por la cuantía económica de 400 euros prevista en el artículo precedente, pues el carácter grave o no de ambos tiene un sentido relativo, en función de la empresa en cuestión. Lo mismo puede decirse respecto de la relevancia del perjuicio producido a la actividad normal de una empresa, negocio o Administración pública, exigido para el tipo agravado de sabotaje de sistemas informáticos por el artículo 264 bis CP.

Por último, la naturaleza inmaterial de la información hace que un posible acceso a o apoderamiento de esta pueda derivar en un delito de espionaje, en un delito de daños o en ambos a la vez. En estas situaciones la dimensión subjetiva del autor juega un papel crucial, de forma que si este persigue desentrañar su contenido para un posible aprovechamiento de la información estaremos ante el primero, si solo quiere destruirla, ante el segundo, y si pretende ambas cosas, se dará una relación concursal entre ambos. Cómo sea dicha relación dependerá del caso concreto ante el que nos encontremos, pero siempre habrá que tener presente el citado elemento para deslindar correctamente los distintos supuestos que puedan tener lugar.

6. *Tabla de jurisprudencia citada*

Tribunal, Sala y Fecha	*Ar.*	*Magistrado Ponente*	*Partes*
SAP Barcelona, 8ª, 04.11.2002	*ARP\2003\221*	*Jesús María Barrientos Pacho*	*Canal Satélite Digital, S.L. c. Asociación Fonográfica y Videográfica Española*
SAP Tarragona, 2ª, 04.04.2003	*JUR\2003\210233*	*Xavier Nouvilas Puig*	*Seric Informática, S.L. c. Héctor*
SJP León, 1ª, 09.02.2004	*ARP\2006\662*	*Ignacio Javier Ráfols Pérez*	*Canal Satélite Digital, S.L. c. Agustín*
SJP Terrassa, 1ª, 01.02.2006	*JUR\2006\113871*	*Desconocido*	*Cornelio c. Luis Ángel*
SAP Barcelona, 2ª, 09.03.2006	*JUR\2006\227208*	*Javier Arzua Arrugaeta*	*Blue Merlin, S.L. c. Milagros*
SAP Sevilla, 7ª, 30.12.2011	*ARP\2012\305*	*Esperanza Jiménez Mantecón*	*Freelan Consultoría y Servicios, S.L. c. Argimiro y Jerónimo*
AAP Barcelona, 2ª, 18.07.2012	*JUR\2012\403963*	*Jaume Rodes Ferrández*	*SGA Information Management, S.A. c. Erica*

SAP Madrid, 6ª, 03.06.2013	*JUR\2013\207748*	*Pedro Javier Rodríguez González-Palacios*	*Remedios c. Patricio*
SAP Madrid, 5ª, 23.10.2015	*JUR\2015\274182*	*Jesús María Hernández Moreno*	*Taisa Syvalue, S.L. c. Narciso*

7. Bibliografía

ANARTE BORRALLO (2002), «Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código Penal», *Jueces para la Democracia*, (43), pp. 50 ss.

———— (2001), «Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información», *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, (1), pp. 191 ss.

ANDRÉS DOMÍNGUEZ (2015), «XXXI. Reformas en daños», en QUINTERO OLIVARES (dir.), *Comentario a la reforma penal de 2015*, Thomson Reuters Aranzadi, Pamplona, pp. 539 ss.

ASÚA BATARRITA (1993), «El daño patrimonial en la estafa de prestaciones unilaterales (subvenciones, donaciones, gratificaciones). La teoría de la frustración del fin», *Anuario de Derecho penal y Ciencias penales*, t. 46, (1), pp. 81 ss.

BAJO FERNÁNDEZ (1978), *Derecho penal económico aplicado a la actividad empresarial*, Civitas, Madrid.

BAJO FERNÁNDEZ/BACIGALUPO SAGGESE (2010), *Derecho penal económico,* 2ª ed., Editorial Universitaria Ramón Areces, Madrid.

BAJO FERNÁNDEZ *et al.* (1993), *Manual de Derecho Penal. Parte Especial. Delitos patrimoniales y económicos,* 2ª ed., Editorial Centro de Estudios Ramón Areces, Madrid.

BOCKELMANN (1952), «Zum Begriff des Vermögensschadens beim Betrug», *Juristen-Zeitung,* pp. 461 ss.

CARRASCO ANDRINO (1998), *La Protección Penal del Secreto de Empresa*, Cedecs Editorial, Barcelona.

CASTRO CORREDOIRA/VÁZQUEZ-PORTOMEÑE SEIJAS (2015), «La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP», en GONZÁLEZ CUSSAC (dir.), *Comentarios a la reforma del Código penal de 2015*, 2ª ed., Tirant lo Blanch, Valencia, pp. 825 ss.

CASTRO MORENO (2006), «El Derecho penal español ante el espionaje industrial y el secreto de empresa (artículos 278-280 CP)», *Rivista Trimestrale di Diritto penale dell'Economia*, pp. 17 ss.

CORCOY BIDASOLO (2015), «Capítulo IX. De los daños», en CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código penal. Reforma LO 1/2015 y 2/2015*, Tirant lo Blanch, Valencia, pp. 926 ss.

CORCOY BIDASOLO/MIR PUIG (2011), «Capítulo IX. De los daños», en CORCOY BIDASOLO/MIR PUIG (dirs), *Comentarios al Código penal. Reforma LO 5/2010,* Tirant lo Blanch, Valencia, pp. 584 ss.

DE LA MATA BARRANCO (1994), *Tutela penal de la propiedad y delitos de apropiación (El dinero como objeto material de los delitos de hurto y apropiación indebida)*, PPU S.A., Barcelona.

DE LA MATA BARRANCO/HERNÁNDEZ DÍAZ (2009), «El delito de daños informáticos: una tipificación defectuosa», *Estudios Penales y Criminológicos*, vol. XXIX, pp. 311 ss.

DÍEZ RIPOLLÉS (2016), *Derecho Penal Español. Parte General*, 4ª ed., Tirant lo Blanch, Valencia.

DÍEZ-PICAZO/GULLÓN (2015), *Sistema de Derecho Civil*, t. I, Vol. III, Derechos reales en general, 8ª ed., Tecnos, Madrid.

DOVAL PAÍS (2008), «La intimidad y los secretos de empresa como objetos de ataque por medios informáticos», *Eguzkilore: Cuadernos del Instituto Vasco de Criminología*, (22), San Sebastián, pp. 89 ss.

ESTRADA I CUADRAS (2016), *Violaciones de secreto empresarial. Un estudio de los ilícitos mercantiles y penales*, Atelier, Barcelona.

FARALDO CABANA (2009), *Las Nuevas Tecnologías en los Delitos contra el Patrimonio y el Orden Socioeconómico*, Tirant Lo Blanch, Valencia.

FERNÁNDEZ SÁNCHEZ (2000), *Protección penal del secreto de empresa*, Colex, Madrid.

FERNÁNDEZ TERUELO (2011), *Derecho penal e internet,* Lex Nova, Valladolid.

GALÁN CORONA (2011), «Artículo 13. Violación de secretos», en BERCOVITZ RODRÍGUEZ-CANO, *Comentarios a la Ley de Competencia Desleal*, Thomson Reuters Aranzadi, Navarra, pp. 351 ss.

GALLEGO SOLER (2002), *Responsabilidad penal y perjuicio patrimonial*, Tirant lo Blanch, Valencia.

GARCÍA ARÁN (1998), *El delito de hurto*, Tirant lo Blanch, Valencia.

GÓMEZ INIESTA (2007), «Artículo 263», en ARROYO ZAPATERO *et al.* (dirs), *Comentarios al Código penal*, Iustel, Madrid, pp. 590 ss.

GÓMEZ RIVERO (2010), *Nociones fundamentales de derecho penal. Parte especial*, Tecnos, Madrid.

GÓMEZ SEGADE (1974), *El secreto industrial (Know-how). Concepto y Protección*, Tecnos D.L., Madrid.

GONZÁLEZ RUS (1999), «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», *Revista Electrónica de Derecho Penal y Criminología*, 01-14.

GUTIÉRREZ FRANCÉS (1996), «Delincuencia económica e informática en el nuevo Código penal», *Cuadernos de derecho judicial*, Consejo General del Poder Judicial, Madrid, pp. 247 ss.

HERRERA MORENO (2011), «Lección 8ª. Daños», en POLAINO NAVARRETE (dir.), *Lecciones de Derecho penal. Parte especial*, Tecnos, Madrid, pp. 133 ss.

HÖRNLE (2012), «Subsidiariedad como principio limitador. Autoprotección», en VON HIRSCH *et al.* (ed. alemana) y ROBLES PLANAS (ed. española), *Límites al Derecho penal. Principios operativos en la fundamentación del castigo*, Atelier, Barcelona, pp. 87 ss.

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (2016), «Guía de almacenamiento seguro de la información», *online* en https://www.incibe.es.

LÓPEZ GARRIDO/GARCÍA ARÁN (1996), *El Código penal de 1995 y la voluntad del legislador. Comentario al texto y al debate parlamentario,* Eurojuris, Madrid.

MARTÍNEZ-BUJÁN PÉREZ (2010), *Delitos relativos al secreto de empresa*, Tirant Lo Blanch, Valencia.

MIR PUIG (2016), *Derecho penal. Parte general*, 10ª ed., Reppertor, Barcelona.

MORALES PRATS (2016), «Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en QUINTERO OLIVARES (dir.)/MORALES PRATS (coord.), *Comentarios a la Parte Especial del Derecho Penal*, 10ª ed., Aranzadi – Thomson Reuters, Navarra, pp. 429 ss.

MORALES PRATS/MORÓN LERMA (2016), «Artículo 278», en QUINTERO OLIVARES (dir.) / MORALES PRATS (coord.), *Comentarios a la Parte Especial del Derecho Penal*, 10ª ed., Aranzadi – Thomson Reuters, Navarra, pp. 844 ss.

MORÓN LERMA (2007), «Quiebras de la privacidad en escenarios digitales: Espionaje industrial», *Eguzkilore*, (21), pp. 117 ss. *online* en http://www.ehu.eus/es/web/ivac.

———— (2002), *El secreto de empresa. Protección penal y retos que plantea ante las nuevas tecnologías*, Aranzadi, Pamplona.

———— (2002), *La tutela penal del secreto de empresa, desde una teoría general del bien jurídico*, tesis doctoral, Universidad Autónoma de Barcelona.

MUÑOZ CONDE (2015), *Derecho penal. Parte especial,* 20ª ed., Tirant lo Blanch, Valencia.

ORTS BERENGUER/ROIG TORRES (2001), *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia.

OTTO (1970), *Die Struktur des strafrechtlichen Vermögensschutzes*, Duncker & Humblot, Berlin.

PICOTTI (2008), «La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale», *Diritto penale e processo*, 6/2008, pp. 696 ss.

———— (1986), «La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati», *Diritto dell'informazione e dell'informatica*, pp. 969 ss.

PRATS (1997), «Descubrimiento y revelación de secretos de empresa en el Código penal de 1995», en DEL ROSAL BLASCO, *Delitos relativos a la Propiedad Industrial, al Mercado y a los Consumidores*, CGPJ, Madrid, pp. 169 ss.

RIBAGORDA GARNACHO (1996), «Seguridad de las tecnologías de la información», *Cuadernos de Derecho judicial* (Ejemplar dedicado a: Ámbito jurídico de las tecnologías de la información), Consejo General del Poder Judicial, pp. 307 ss.

ROBLES PLANAS/PASTOR MUÑOZ (2015), «Tema 12. Delitos contra el patrimonio (III)», en SILVA SÁNCHEZ (dir.), *Lecciones de Derecho penal. Parte especial*, Atelier, Barcelona, 2015, pp. 277 ss.

ROMEO CASABONA (2004), *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia.

SANTANA VEGA (2015), «Sección 3ª. De los delitos relativos al mercado y a los consumidores", en CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal.* Tirant Lo Blanch, Valencia, pp. 975 ss.

SERRANO GÓMEZ/SERRANO MAÍLLO (2010), *Derecho penal. Parte especial*, 15ª ed., Dykinson, Madrid.

SERRANO-PIEDECASAS/DEMETRIO CRESPO (2010), *Cuestiones actuales de Derecho penal empresarial*, Colex, Madrid.

TIEDEMANN (2012), *Manual de Derecho Penal Económico. Parte Especial*, Editora y Librería Jurídica Grijley, Perú.

ZUGALDÍA ESPINAR (1988), *Delitos contra la propiedad y el patrimonio*, Akal, Madrid.