LA AMENAZA DE LAS NUEVAS TECNOLOGÍAS EN LOS NEGOCIOS: EL CIBERESPIONAJE EMPRESARIAL

THE THREAT OF NEW TECHNOLOGIES IN BUSINESS: CORPORATE CYBERESPIONAGE

Premio de Artículos Jurídicos «García Goyena»
XVII Edición
Primer premio

Carmen Rocío Fernández Díaz

Pseudónimo: *Policarpa Salavarrieta*

Resumen: La globalización de los mercados y la constante evolución de las nuevas tecnologías convierten cada vez más a la empresa en objeto de ataques cibernéticos. Uno de los más frecuentes y de los que más daños generan es el ciberespionaje, que conlleva una violación de la propiedad inmaterial de una empresa. El correcto abordaje de este delito, adaptado a las diferentes modalidades comisivas, en constante evolución, teniendo en cuenta sus diversas finalidades y considerando aristas aún desconocidas en nuestro país, como la inteligencia competitiva, constituye un auténtico desafío para el Derecho penal español. El presente trabajo estudia este delito en nuestro país, desde un punto de vista crítico para detectar sus posibles carencias y la necesidad de encontrar soluciones a las mismas, acudiendo para ello a la legislación, la jurisprudencia y la doctrina españolas, pero también considerando otras experiencias nacionales, como la de Italia, Alemania o Estados Unidos.

Palabras clave: Espionaje, ciberespionaje, empresa, ciberdelincuencia, nuevas tecnologías.

Abstract: Due to the market globalization and the constant evolution of new technologies, companies become more often the object of cyber attacks. One of the most frequent and most damaging is cyberespionage, which involves a violation of the intangible property of a company. The correct approach to this crime, adapted to the different manners in which it is committed, in constant evolution, constitutes an authentic challenge for Spanish criminal law, if we consider its different purposes and areas that are still unknown in our country, such as competitive intelligence. The present work studies this crime in our country from a critical point of view to detect its possible failures, and also the need to find solutions for them. To do so, therefore have been consulted the Spanish legislation, case-law and doctrine, but also analyzed other national experiences, like the one in Italy, Germany or the United States.

Keywords: Espionage, cyberespionage, corporation, cyber delinquency, new technologies.

I. INTRODUCCIÓN

Las nuevas tecnologías de la información y la comunicación (TIC) se imponen en prácticamente todos los ámbitos de la vida diaria y a estas alturas del siglo XXI, constituye la regla y no la excepción el que la comisión de ciertos comportamientos delictivos tenga lugar casi exclusivamente a través de ellas.

Uno de esos ámbitos viene dado por la actividad empresarial cotidiana, donde las TIC tienen un indudable impacto. En las sociedades modernas la empresa tiene un papel cada vez más importante

en el tejido económico[1] y en nuestro país especialmente la pequeña y mediana empresa, que constituye el 99,88% del tejido empresarial español[2]. Actualmente es impensable e incluso imposible que las ingentes cantidades de información que se manejan en el mercado por parte de sus agentes principales se almacenen en soportes no electrónicos, cuya intervención en dicha actividad resulta indispensable para su propia existencia. Además de lo anterior, son cada vez más las empresas que, sin una sede física, se instalan en el espacio virtual, realizándose por estos medios la completa interacción con sus clientes.

La «digitalización» de la sociedad fomenta el que la empresa constituya, como ya pusiera de manifiesto Bernd Schünemann, un factor que genera criminalidad, tanto en relación a delitos económicos que se cometen a partir de una empresa (*criminalidad de empresa*) como respecto de aquellos que se cometen por colaboradores de la empresa a esta o a otros de sus colaboradores (*criminalidad en la empresa*)[3].

Todo lo anterior hace especialmente necesaria la atención a un tipo delictivo como el que aquí se estudia. El espionaje no es un delito nuevo ni tampoco se ciñe estrictamente al ámbito empresarial, pues ha tenido una gran relevancia a lo largo de la historia sobre todo en relación a los secretos de Estado y a la seguridad nacional. Sin embargo, el que aquí interesa es el que tiene la empresa como escenario, entendida en sentido físico y/o virtual, y que radica en la obtención ilegítima de los secretos que le pertenecen, constituidos por información empresarial reservada, de difícil ubicación en las categorías tradicionales relativas a los bienes inmateriales, cuyo estudio especializado, con carácter previo a la tipificación del delito, ha sido realizado casi exclusivamente por autores mercantilistas.

---

[1] El Instituto Nacional de Estadística (INE) recogía en el año 2017 más de tres millones de empresas distribuidas en un total de hasta ochenta tipos de actividades económicas en nuestro país. Pueden consultarse estos datos en http://www.ine.es/jaxiT3/Datos.htm?t=3954

[2] Así, según el Directorio Central de Empresas (DIRCE), en datos ofrecidos por el Ministerio de Industria, Energía y Turismo en febrero de 2016, casi la totalidad del conjunto empresarial español, el 99,88%, lo que equivale a 3.178.408 unidades productivas, está constituido por pequeñas y medianas empresas (PYME). Puede consultarse dicha información en el siguiente enlace: http://www.ipyme.org/Publicaciones/ESTADISTICAS-PYME-2015.pdf

[3] SCHÜNEMANN, B.: «Cuestiones básicas de dogmática jurídico-penal y de política criminal acerca de la criminalidad de empresa», *Anuario de derecho penal y ciencias penales*, Tomo 41, Fasc/Mes 2, 1988, págs. 529-530.

Sin embargo, el interés del Derecho penal por esta figura delictiva está justificado hoy más que nunca, en la medida en que el clásico espionaje industrial que tenía lugar entre competidores de un mismo sector pertenecientes incluso a una misma zona y cuya comisión tenía lugar predominantemente mediante el robo de documentación en formato papel, se torna en nuestros días en una actividad sin fronteras, de contornos indefinidos[4], que abarca además del llamado secreto industrial, información reservada de naturaleza comercial y constituyendo la vía de ataque por antonomasia mecanismos que emplean de una u otra forma artificios técnicos y medios telemáticos, dando lugar al nacimiento de una nueva forma de conducta, el llamado ciberespionaje.

Muestra de la importancia de este tipo de criminalidad son los datos que ofrecen diferentes organizaciones en relación al ciberespionaje económico. Por un lado, un estudio sobre el impacto económico de este tipo de criminalidad, elaborado por la principal compañía de seguridad informática a nivel mundial, apunta que el espionaje que se comete a través de medios informáticos constituye la causa de las pérdidas económicas más importantes que se derivan de la ciberdelincuencia[5]. Por otro lado, el resumen ejecutivo del Centro Criptológico Nacional (CCN-CERT IA-16/17) pone de relieve que el ciberespionaje económico constituye la principal amenaza para el mundo occidental y que este experimentó un importante crecimiento en 2016[6].

Sin embargo, existe una importante cifra negra en esta materia debido principalmente a dos factores: en primer lugar, la dificul-

[4] Como afirma GONZÁLEZ CUSSAC, J.L.: «Tecnocrimen», en GONZÁLEZ CUSSAC, J.L. / CUERDA ARNAU, M.L. (dirs.): *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant lo Blanch, Valencia, 2013, págs. 224-225, la ciberdelincuencia trae consigo ciertos problemas en la medida en que en las comunicaciones telemáticas, las fronteras se tornan inexistentes y los espacios pierden su materialidad, lo cual hace que se conviertan en cuestiones problemáticas, entre otras, la determinación del lugar o momento de comisión de los delitos, los sujetos responsables de estos o la jurisdicción competente.

[5] Informe «The economic impact of cybercrime and cyber espionage» (pág. 8), elaborado por el Centro para Estudios Estratégicos e Internacionales (*Center for Strategic and International Studies*), a cargo de la empresa de seguridad informática McAfee, en el año 2013. Recientemente ha anunciado que sigue aumentando sus esfuerzos por combatir este delito (YOUNG, C.: McAfee Raises the Stakes Against Cyberespionage», *McAfee*, 3/5/2017 - https://securingtomorrow.mcafee.com/executive-perspectives/mcafee-raises-stakes-cyberespionage/-).

[6] Puede accederse al citado documento en el siguiente enlace: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2221-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017-resumen-ejecutivo-1.html

tad del titular para percatarse de haber sido víctima de un comportamiento contra secretos de empresa, dada la posibilidad de pasar inadvertida dicha conducta cuando se trata de reproducir bienes inmateriales[7]; y, en segundo lugar, los riesgos que supone para la empresa iniciar un procedimiento judicial en el que probablemente termine por perder la información empresarial el valor que le restaba tras dicho comportamiento ilícito[8], a lo cual se suma la desacreditación que puede sufrir la empresa por ponerse de manifiesto la vulnerabilidad de sus medidas de seguridad.

El delito de espionaje empresarial no se introdujo en nuestro ordenamiento jurídico-penal hasta el año 1995[9], aunque en sede civil se reguló cuatro años antes, cuando la Ley 3/1991, de 10 de enero, de Competencia Desleal (LCD), en su artículo 13, tras reputar como desleal en su párrafo primero «*la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales…*», previó en el segundo que «*[t]endrán asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo*».

Junto a la regulación extrapenal, la de carácter internacional también ejerció una importante influencia en la tipificación de este delito, como fue el caso del artículo 39.2 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio de 15 de abril de 1994, que más adelante comentaremos. Sin embargo, la preocupación internacional por esta cuestión se

[7] DREYFUSS, R.C. / STRANDBURG, K.J. (eds.): *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*, Edward Elgar, Cheltenham (UK)-Northampton (MA, USA), 2011, pág. xviii. Estas autoras estadounidenses ponen de manifiesto la escasez de datos que existe con los que poder trabajar al no existir registros de secretos de empresa y solo unos pocos indicadores de su importancia económica, a diferencia de lo que ocurre con el sistema de patentes.

[8] Para evitar en la medida de lo posible estas consecuencias, la Directiva (UE) 2016/943, de 8 de junio de 2016, del Parlamento Europeo y del Consejo, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, prevé en sus considerandos 7 y 24 y en su artículo 9, un régimen de protección ante denuncia en proceso judicial, intentando evitar así la cifra negra que existe por la desprotección a la que se somete al titular del secreto en este momento respecto de sus bienes inmateriales.

[9] La inclusión del espionaje empresarial como figura delictiva sí estuvo prevista en el Proyecto alternativo alemán de 1977, cuyo §180 apartado 3 castigaba a quien «mediante un artificio o burlando dispositivos de protección accede a un secreto comercial o industrial para revelarlo a otro o para utilizarlo económicamente» (LAMPE/LENCKNER/STREE/TIEDEMANN/WEBER: *Alternativ-Entwurf eines Strafgesetzbuches. Besonderer Teil. Straftaten gegen die Wirtschaft*, Tübingen 1977, pág. 53).

ha acrecentado en los últimos años. Muestra de ello es la Directiva (UE) 2016/943, de 8 de junio de 2016, del Parlamento Europeo y del Consejo, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. En dicho texto se pone el acento en el papel de los secretos de empresa, que son resultado de creaciones intelectuales de las empresas que precisan protección, como impulsores de la innovación y el desarrollo[10]. Estos dos últimos aspectos, junto a la investigación científica y técnica, son considerados factores indispensables para el crecimiento económico de un país y constituyen la base de su progreso y bienestar sociales[11].

Asumiendo la importancia de esta cuestión, el presente trabajo ahonda en ella desde cuatro vertientes. En primer lugar, se estudia su regulación penal, aludiendo al sujeto activo del delito, al objeto de la conducta típica y a esta última, detectando las falencias de la misma y su posible subsanación *de lege lata* o *de lege ferenda*. En segundo lugar, se analizan las modalidades comisivas más frecuentes de ciberespionaje cuya peculiaridad es un acceso ilícito telemático. En tercer lugar, se alude a la inteligencia competitiva, técnica de obtención de información empresarial de carácter lícito, como riesgo para la propiedad inmaterial de la empresa frente al espionaje. Y, en cuarto lugar, se enumeran las posibles finalidades directas del espionaje así como las de carácter complementario, identificando ciertas lagunas que necesitarían cubrirse por el legislador para dotar de una protección integral a la empresa contra este tipo de delincuencia.

En definitiva, se aborda el delito de ciberespionaje desde sus diversas aristas para ofrecer una visión completa del mismo y afrontar así uno de los mayores desafíos del siglo XXI.

[10] Considerando (3) de la Directiva (UE) 2016/943, de 8 de junio de 2016, del Parlamento Europeo y del Consejo, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

[11] Así lo ha puesto de manifiesto el Ministerio de Economía y Competitividad en la llamada «Estrategia española de ciencia y tecnología y de innovación 2013-2020» (pág. 8). A dicho texto puede accederse en el siguiente enlace: http://www.idi.mineco.gob.es/stfls/MICINN/Investigacion/FICHEROS/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf

II. REGULACIÓN PENAL DEL CIBERESPIONAJE EMPRESARIAL

El ciberespionaje se castiga en el Código penal español en el artículo 278.1, el cual establece la aplicación de una pena de dos a cuatro años de prisión o de doce a veinticuatro meses de multa a «El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197…». Este último precepto, para el caso de los secretos relativos al ámbito de la intimidad, alude también al apoderamiento de ciertos soportes y a la interceptación de las telecomunicaciones y la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación. Antes de adentrarnos en el análisis de la conducta típica relativa al ciberespionaje, es necesario hacer alusión a dos cuestiones fundamentales de su regulación, como son, el sujeto activo del delito y el objeto del mismo, esto es, el secreto de empresa.

El sujeto activo del ciberespionaje puede ser cualquiera, pues al emplear la fórmula genérica «el que» no se exige para ser tal elemento especial y adicional alguno. Sin embargo, quedan fuera del tipo las extralimitaciones de los empleados si, una vez cesada su actividad laboral, siguen accediendo a la información de su empresa con el uso de sus claves, todavía activas[12], pues en estos casos no estamos ante un delito de espionaje, al existir el tipo especial del artículo 279.2 CP, de utilización en provecho propio, en su forma consumada o intentada[13]. Sin embargo, esta interpretación en nada obsta a que el empleado de una empresa pueda ser sujeto activo del

[12] Sin embargo, algunas resoluciones han condenado a estos sujetos que acceden de forma «lícita»a la información empresarial por la vía del artículo 278.1 CP. Así ocurrió en la SAP Tarragona (Sección 2.ª) 127/2003, de 4 de abril, en la que el administrador de sistemas de una empresa, teniendo acceso a datos confidenciales, como las claves de todos los clientes y empleados, se aprovechó de ello, no limitándose solo a entrar en el sistema ajeno, comportamiento que habría quedado impune o comprendido entre los delitos informáticos si había vulnerado para ello alguna medida de seguridad, sino que además copió la información e instaló en su propio ordenador los códigos fuente de programas comerciales pertenecientes a la empresa, siendo condenado por un delito de apoderamiento de los secretos de esta del artículo 278.1 CP.

[13] Son los casos que Morón Lerma llama de apoderamiento «abusivo» (MORÓN LERMA, E.: *La tutela penal del secreto de empresa, desde una teoría general del bien jurídico*, Tesis doctoral Universidad Autónoma de Barcelona, 2002, págs. 544-545, 576 y 597 y ss.).

delito del artículo 278 CP, cuando acceda de forma ilícita a información de esta que no conociera[14].

Por lo que respecta al objeto del ciberespionaje, este viene constituido por los secretos de empresa. Dicho concepto, que incluye toda información de índole industrial y comercial (en especial, las listas de clientes[15]), se define a partir de lo establecido en el artículo 39.2 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC o, en inglés, Acuerdo TRIPS —*Trade-Related aspects of Intellectual Property rights*—)[16] o el 2.1 de la *Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8 de junio de 2016 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas*. Según estos textos de carácter internacional, la información debe cumplir tres requisitos: en primer lugar, esta ha de tener carácter reservado, entendiendo por tal que no sea generalmente conocida ni fácilmente accesible por las personas que pertenecen al círculo donde normalmente aquella se utiliza; en segundo lugar, el titular de la información debe manifestar su voluntad de mantenerla en secreto, adoptando para ello medidas razonables en el caso concreto; y, en tercer lugar, la información tiene que tener un valor empresarial, lo cual dependerá de cada empresa, por lo que incluso las cosas más triviales en apariencia pueden ser calificadas como secreto empresarial, si para su titular tienen valor[17].

De todos estos aspectos, el de mayor relevancia, como se verá, es la adopción de medidas por el titular de la información para su protección, pues estas le confieren a su titular la exclusividad sobre el secreto, frente a la inscripción registral en el caso de los derechos de propiedad industrial. La doctrina ha puesto de manifiesto que a pesar de que las empresas a menudo realizan importantes inversiones para generar ideas y productos, es frecuente que no lo hagan signi-

[14] Este fue el caso de la SAP Barcelona (Sección 8.ª) 271/2016, de 2 de junio, en el que el acusado era el encargado del área de montaje de contenedores de una empresa, sin que su actividad profesional tuviera relación alguna con la información comercial de la que se apoderó.

[15] Para un acercamiento más profundo a esta cuestión, *cfr*. FERNÁNDEZ DÍAZ, C.R.: «La lista de clientes como objeto del secreto empresarial», *Revista Aranzadi Doctrinal*, Núm. 7 (julio de 2016).

[16] 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.

[17] POOLEY, J.H.A.: *Trade Secrets. A guide to protecting Proprietary Business Information*, American Management Association, New York, 1987, pág. 6.

ficativamente en la protección de su valioso capital intelectual[18]. Sin embargo, la idea de autoprotección de la víctima juega aquí un papel importante, pues en ocasiones el Derecho penal no puede intervenir porque al final lo decisivo es que la lesión o peligro del bien jurídico es imputable a que la víctima lo ha posibilitado por no haber adoptado medida alguna[19]. Así pues, en tales casos el hecho es menos grave que cuando el titular del bien ha adoptado medidas[20], que deben dirigirse tanto a terceros ajenos a la empresa, como a sus propios empleados[21].

Pues bien, el ciberespionaje encuentra castigo en la referencia a la interceptación de las telecomunicaciones, la cual, junto a la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, procede del mismo antecedente legislativo, esto es, la regulación de las llamadas «escuchas ilegales». Estas fueron incorporadas al anterior Código penal por la LO 7/1984, de 15 de octubre, mientras que fue la LO 18/1994, de 23 de diciembre, la que finalmente abrió el ámbito típico a la captación de la imagen y a la interceptación de comunicaciones en general[22]. De esta forma, pare-

[18] MARRS, S.: «Inside Story on Trade Secrets: Protective measures are necessary to preserve a company's vital information», *ABA Journal*, Vol. 86, No. 10 (October 2000), pág. 77. Este autor concluye afirmando que las empresas son tan valiosas como el capital intelectual que las distingue de sus competidores.

[19] HÖRNLE, T.: «Subsidiariedad como principio limitador. Autoprotección», en VON HIRSCH, A. / SEELMANN, K. / WOHLERS, W. (ed. Alemana) y ROBLES PLANAS, R. (ed. Española): *Límites al Derecho penal. Principios operatives en la fundamentación del castigo*, Atelier libros jurídicos, Barcelona, 2012, pág. 88. 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» (*ibídem*, pág. 90). En el mismo sentido, MIR PUIR, S.: *Derecho penal. Parte general*, 10.ª edición, editorial Reppertor, Barcelona, 2016, pág. 128.

[20] Los autores del Proyecto alternativo alemán de 1977, al castigar el espionaje empresarial, argumentaban, con razón, que «el Derecho penal tiene que intervenir únicamente en aquellos casos en que el titular del secreto ha hecho todo lo necesario para proteger el secreto y el autor ha quebrado los dispositivos de seguridad exigibles al titular del bien jurídico» (LAMPE/LENCKNER/STREE/TIEDEMANN/WEBER: Alternativ-Entwurf. *Op. cit.,* pág. 55).

[21] Si el empleado conoce la información bajo un compromiso o pacto de confidencialidad y la revela, entraría dentro del tipo del artículo 279.1 CP, pero en todo caso, las medidas deben tomarse en ambas direcciones. Sobre el monitoreo o control de los empleados, *cfr*. CHAN, M.: «Corporate Espionage and Wordplace Trust/Distrust», Journal of Business Ethics, Vol. 42, No. 1 (Jan., 2003), págs. 45-58.

[22] ANARTE BORRALLO, E.: «Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código Penal», en *Jueces para la Democracia*, n.º 43, 2002, pág. 55.

ciera que con la inclusión de ambas modalidades pretendía evitarse la captación ilícita de comunicaciones reservadas en el ámbito empresarial que tuvieran lugar, tanto a través de telecomunicaciones, como de forma presencial, con el elemento común de que para ello se empleaban medios técnicos.

En primer lugar, a pesar de que la introducción de esta conducta se realizó en un momento en el que la forma de comunicación telemática predominante era la telefónica, a principios de los años '90 la sociedad empezó a utilizar internet tal y como lo conocemos actualmente, esto es, como medio de comunicación a distancia. Ello obliga a interpretar este tipo de forma que no se dejen de lado comportamientos típicos que hoy están en auge, y que se relacionan fundamentalmente con el uso de las TIC, lo cual es posible gracias a la redacción en términos amplios, aludiendo en general a las «telecomunicaciones».

En segundo lugar, por lo que respecta al objeto sobre el que recae la conducta de interceptación, como acabamos de mencionar, este se cifra en las *telecomunicaciones*. Por «telecomunicación» puede entenderse actualmente un «sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos»[23]. Esta definición ha cambiado recientemente en el Diccionario de la Lengua Española (en adelante, DLE), siendo la precedente una diferente, según la cual, por aquella se entiende todo «sistema de comunicación telegráfica, telefónica o radiotelegráfica y demás análogos»[24]. En estos casos resulta claro que el precepto alude a comunicaciones que están teniendo lugar exclusivamente a través de un medio de comunicación telemático, esto es, a distancia, y no entre personas que se encuentren en un mismo lugar ni que estén hablando directamente (por ejemplo, en una reunión). De la alusión a las telecomunicaciones, por tanto, se deduce que el escenario donde tiene lugar la acción típica de interceptar, desde el inicio de su ejecución hasta su consumación, es un espacio virtual.

En tercer lugar, es necesario aclarar el sentido de la conducta a la que se refiere el tipo. El término *interceptación* alberga tres acepciones en el DLE[25] que lo definen, en primer lugar, como «apoderarse de algo antes de que llegue a su destino»; en segundo lugar, como «detener algo en su camino»; y, finalmente, como «interrum-

[23] Única acepción del término del Diccionario de la Lengua Española (http://lema.rae.es/drae/?val=telecomunicaci%C3%B3n).

[24] Se ha indagado en el momento y el motivo de su modificación, sin haber obtenido un resultado de ello.

[25] A ellas puede accederse a través del siguiente enlace: http://dle.rae.es/?id=-LsigOEU

pir, obstruir una vía de comunicación». La doctrina ha estimado que la referencia típica debe ser interpretada en el sentido de la primera definición, pues las otras dos no encajan en una concepción teleológica del precepto. Así entendida la interceptación, esta conllevaría un apoderamiento o captación previos a la llegada de cierta información a su destino, ya sea impidiendo que esta finalmente lo haga o no y, por tanto, debiendo de tratarse de comunicaciones que se están llevando a cabo[26]. Dicha interpretación no es incompatible con la que Castro Moreno realiza del verbo típico, definiéndolo como «introducirse en la comunicación mediante el empleo de artificios técnicos, descubriendo su contenido», sin rechazar por ello, como propugna, las definiciones gramaticales del término[27].

Sin embargo, en mi opinión, estas interpretaciones no captan la esencia del comportamiento que aquí debería castigarse, por lo que dejarían fuera del tipo otras formas de hacerse con la información empleando internet como medio. Así, por un lado, deberían entenderse incluidos *de lege lata* en esta modalidad típica no solo aquellos apoderamientos que se realicen sobre la información antes de que esta llegue a su destino, como indica su definición, sino también aquellos que se llevan a cabo sobre la que está ya almacenada por un usuario en equipos informáticos, cuentas de correo electrónico, teléfonos móviles, relojes o tabletas electrónicas, discos duros externos o en servidores como la nube, entre otros. Esta exégesis de carácter amplio viene avalada por el artículo 3 del *Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*, y publicado en el BOE con fecha de 17 de septiembre de 2010, que constituye el primer instrumento normativo en el ámbito europeo desde la perspectiva penal sustantiva[28], así como por el artículo 6 de 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*[29] y por la que se sustituye la Decisión Marco

[26] De esta opinión son ANARTE BORRALLO, E.: Consideraciones sobre los delitos de descubrimiento. *Op. cit*., pág. 56; ORTS BERENGUER, E. / ROIG TORRES, M.: *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch «colección de delitos», Valencia, 2001, pág. 25. En sentido contrario, MORALES PRATS, F.: «Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en QUINTERO OLIVARES, G. (dir.) / MORALES PRATS, F. (coord.): *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi-Thomson Reuters, Navarra, 2016, pág. 410.

[27] CASTRO MORENO, A.: «El derecho penal español ante el espionaje industrial y el secreto de empresa (artículos 278-280 CP)», en *RTDPE (Rivista Trimestrale di Diritto penale dell'Economia)*, I-2/2006, pág. 50.

[28] GONZÁLEZ CUSSAC, J.L.: «Tecnocrimen». *Op. cit.*, pág. 235.

[29] Diario Oficial de la Unión Europea L 218/8, 14.8.2013.

2005/222/JAI del Consejo, de 24 de febrero, relativa a los ataques contra los sistemas de información. En virtud de estos dos textos internacionales, la interceptación ilícita por medios técnicos de datos informáticos se extiende no solo a las comunicaciones entre un sistema informático y otro, sino también dentro de ellos. Por otro lado, dicho comportamiento no supone exactamente, como afirma Castro Moreno, la introducción y descubrimiento de una comunicación, sino que puede que no llegue a descubrirse o a conocerse la información contenida, siendo lo relevante a efectos de la consumación del tipo que se acceda a la información y que esta pase a la esfera de dominio del sujeto activo. Por estos motivos, *de lege lata*, hay que interpretar la interceptación en un sentido amplio, como toda obtención de información que se encuentra almacenada digitalmente o que proviene de comunicaciones telemáticas, usando para ello medios ilícitos que funcionan a través de una red de telecomunicación. Dichos medios, que en la mayoría de ocasiones presentan un carácter subrepticio y engañoso, son ejemplos claros de accesos ilícitos a la esfera de exclusión del titular de la información empresarial.

III. MODALIDADES COMISIVAS DEL CIBERESPIONAJE

A. El acceso ilícito como presupuesto típico del ciberespionaje

El acceso ilícito constituye el presupuesto típico del espionaje empresarial, debiendo producirse de forma remota o telemática en el caso del ciberespionaje, esto es, en el escenario virtual y sin acción física o directa sobre el equipo atacado. Sin embargo, no es suficiente con que este concurra para entender que se ha consumado el delito, siendo necesario algo más[30], esto es, que el sujeto efectivamente tenga el dominio sobre la información reservada. Esta interpretación se refuerza si miramos a otros tipos penales, donde el legislador ha querido castigar expresamente el mero acceso.

En primer lugar, ello ocurre especialmente en los delitos contra la intimidad, donde se contienen gran parte de los tipos que castigan los ataques a sistemas informáticos, por lo que su referencia en este

[30] El verbo «apoderarse» ha sido definido por el Diccionario de la Lengua Española como «poner algo en poder de alguien o darle la posesión de ello» o «hacerse dueño de algo, ocuparlo, ponerlo bajo su poder». Así lo establece el DLE en la segunda y tercera acepciones, respectivamente, del verbo «apoderar». Si bien la segunda es considerada anticuada por la propia RAE, la tercera es la que adquiere pleno sentido en el caso que nos ocupa.

punto resulta obligada. Por un lado, tal es el caso del *artículo 197.2 CP*, que tipifica el acceso por cualquier medio y sin autorización a ficheros, soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado. Por otro lado, especial mención merece en la distinción entre acceso y apoderamiento el *artículo 197 bis CP*, donde se sanciona al que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o se lo facilite a otro, al conjunto o a una parte de un sistema de información o se mantenga en él contra la voluntad de quien tenga el legítimo derecho a excluirlo. Este precepto castiga la llamada intrusión informática o «*hacking*», modificado en la reforma llevada a cabo por la LO 1/2015, de 30 de marzo, y en él puede verse claramente cómo la vulneración de las medidas de seguridad que impiden el acceso a un sistema informático y la falta de autorización para acceder son los elementos que definen el tipo. Este precepto ya estaba previsto antes de la reforma en el artículo 197.3 CP, solo que el legislador de 2015 quiso darle mayor autonomía por considerar que este tenía un objeto de tutela distinto[31]. Ya antes de la modificación existían también resoluciones de nuestros tribunales que marcaban claramente la diferencia entre el mero acceso y la conducta de apoderamiento. Tal es el caso de la SAP Murcia (Sección 3.ª), 88/2015, de 20 de febrero, en el que se condenó por un delito del artículo 197.3 CP a la empleada de una empresa que accedió intencionadamente de forma ilegítima a correos de diversas trabajadoras de la mercantil y, por tanto, a datos y programas contenidos en el sistema informático propio de aquella, pero sin que quedara acreditado el apoderamiento, interceptación, utilización o modificación de estos por parte de la acusada. En sentido similar se pronunció también la SAP Madrid (Sección 2.ª), 329/2015, de 27 de abril, que expresamente afirmó que con el delito del artículo 197.3 CP, que introdujo el mero intrusismo, conocido también como «hacking blanco», se castiga el acceso no consentido, es decir, el solo hecho de saltarse

[31] Así, el propio Preámbulo de la Ley, en su apartado XIII, puso de manifiesto que para transponer la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información, era necesario distinguir los supuestos de revelación de datos que afectaban directamente a la intimidad personal, del acceso a otros datos o informaciones que podían afectar más bien a la privacidad, pero que no estaban referidos directamente a la intimidad personal. También en este sentido, en el ordenamiento jurídico italiano, PICOTTI, L.: «Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale», en *Diritto dell'internet*, n.2/2005, pág. 193; el mismo: «Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati», en PICOTTI, L. (dir.): *Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, Padova, 2004, págs. 80 y ss..

las barreras de seguridad informáticas, sin necesidad de realizar acción posterior alguna.

En segundo lugar, también el legislador penal ha querido castigar el simple acceso en el *artículo 415 CP*, tanto si lo efectúa el propio sujeto activo del delito, que es la autoridad o funcionario público, como si este se permite, respecto a documentos secretos cuya custodia le esté confiada por razón de su cargo, a sabiendas y sin la debida autorización.

En tercer lugar, asimismo el *artículo 603 CP* castiga, entre otras conductas, la de abrir sin autorización la correspondencia o documentación legalmente calificada como reservada o secreta, relacionada con la defensa nacional, por quien la tenga en su poder por razones de su cargo o destino.

Por tanto, como puede observarse, el legislador ha querido exigir algo más en el ciberespionaje respecto a estos preceptos, en los que el adelantamiento de las barreras de protección llega a castigar una mera entrada o introducción en los soportes donde se contiene la información. Hay autores que han equiparado dicho acceso, entrada o introducción con visualizar o escuchar la información[32]. Sin embargo, lo que sucede es que dada la inmaterialidad de esta, algunas formas comisivas dan lugar a que el acceso ya pueda llevar consigo el apoderamiento. Así ocurre si de dicha visualización o escucha, el sujeto llega a conocer el secreto o a retenerlo mentalmente, pudiendo disponer de él con posterioridad, no dándose ya un mero acceso. Lo relevante es que este último supone una vulneración de las medidas de protección adoptadas por el titular de la información para mantener su reserva, pero no basta con dicha vulneración, si finalmente el sujeto no la pone bajo su control.

B. Medios subrepticios de acceso a sistemas de información ajenos

Partiendo del necesario acceso ilícito que precede a la obtención o dominio de la información, aquel puede tener lugar de diversas maneras. Las más frecuentes formas de comunicación telemática actualmente son el teléfono y las redes informáticas, ya sean internas (como intranet) o externas (como internet). Como medio de ataque

[32] CARBONELL MATEU, J.C. / GONZÁLEZ CUSSAC, J.L.: «Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en VIVES ANTÓN, T.S.: *Comentarios al Código Penal de 1995*, Tirant lo Blanch, Valencia, 1996, pág. 1001.

a la primera de ellas hay que destacar el llamado «pinchazo». En las segundas, la variedad de métodos aumenta vertiginosamente y constituyen el medio que mayor protagonismo ha adquirido, ofreciendo técnicas especialmente sofisticadas para almacenar información y acceder a ella de modo ilegítimo, dando lugar así a la forma más común de ciberespionaje[33].

Actualmente toda empresa tiene presencia en internet y la mayoría de sus datos digitalizados, lo cual aumenta exponencialmente los riesgos de ataque. Las actuales tendencias como la migración de los datos a la nube y la salida de la red interna de la empresa hacia los aparatos móviles hacen que la tarea de proteger la propiedad intelectual de una empresa sea mucho más difícil[34], lo cual se agrava en el caso de las pequeñas y medianas empresas, que como se ha dicho, predominan en España, normalmente vinculadas a una actividad concreta y menos tendentes a prestar atención al desarrollo de un efectivo programa de ciberseguridad[35].

Entre las formas de comisión del ciberespionaje que pueden darse en la actualidad cabe destacar algunas como los programas rastreadores o analizadores de paquetes, más conocidos con el término anglosajón de «*sniffers*», cuya instalación permite la captura de tramas que circulan por la red a través de un programa que se ejecuta en una máquina conectada a ella o bien a través de un dispositivo que se engancha directamente al cableado[36]; también la llamada minería de datos o «*data mining*», que consiste en una tecnología empleada para descubrir información oculta y desconocida que resulta potencialmente útil, y que se obtiene a partir de fuentes

[33] El ciberespionaje puede tener lugar en muchos ámbitos, no solo en el empresarial. Si hablamos de ciberespionaje económico, este tiene diferentes connotaciones en función del sujeto al que se dirige, que pueden ser individuos, organizaciones empresariales o Estados. Una definición global del citado concepto puede ser la propuesta por Larriba Hinojar, quien lo entiende como «la actividad sistemática de obtención clandestina de información protegida por su propietario (…) a través del empleo de sistemas o redes interconectadas y su infraestructura asociada, fundamentalmente Internet» (LARRIBA HINOJAR, B.: «Ciberespionaje económico: Una amenaza real para la Seguridad Nacional en el siglo XXI», en GONZÁLEZ CUSSAC, J.L. / CUERDA ARNAU, M.L. (dirs.): *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant lo Blanch, Valencia, 2013, pág. 329).

[34] BRADLEY, T.: «McAfee: Corporate Espionage is the Currency of Cybercrime», *PcWorld*, 28 de marzo de 2011 (http://www.pcworld.com/article/223483/mcafee_corporate_espionage_is_the_currency_of_cybercrime.html).

[35] COWPERTHWAIT, T.S.: «Businesses Must Protect Against Cyber-Espionage», en *Connecticut Law Tribute*, vol. 37, n.º 11, 2011, pág. 1.

[36] FARALDO CABANA, P.: *Las Nuevas Tecnologías en los Delitos contra el Patrimonio y el Orden Socioeconómico*, Tirant Lo Blanch, Valencia, 2009, pág. 246.

de información de la propia empresa, a través de técnicas estadísticas de análisis de grandes bases de datos[37]; o algunas que se realizan a través de programas o softwares maliciosos (*malwares*), perpetradas por piratas informáticos o «*hackers*», que permiten hacerse con información que se encuentra en el ciberespacio y que constituirían la interceptación de las telecomunicaciones cuando se realicen de forma remota. Ahora bien, estas conductas, como ya se ha comentado, no pueden consistir solamente en un acceso ilícito a la información, pues si así fuera estaríamos ante un delito de mero acceso o intrusismo informático (*hacking*), previsto en el artículo 197 bis CP. Es necesario, además, que de dicho acceso se derive la obtención de información que tenga las características de un secreto de empresa. Entre este tipo de comportamientos, los más destacados medios de ataque actualmente son los siguientes:

1. Troyanos

Son un tipo de software malicioso que se oculta en programas legítimos como pueden ser documentos de trabajo de una empresa o imágenes digitales, para así proporcionar un acceso no autorizado al sistema infectado. Este tipo de virus se ha especializado en el robo de credenciales bancarias y presenta varias tipologías a través de las cuales puede ejecutarse la interceptación. Así, en primer lugar, se encuentran las puertas traseras o «*backdoors*», que permiten un acceso remoto a la totalidad del equipo informático, pudiendo el sujeto activo realizar cualquier tarea en él; en segundo lugar, otra tipología son los captateclas o «*keyloggers*», un tipo de troyano que registra las pulsaciones realizadas con el teclado y que permite averiguar contraseñas u otro tipo de información que haya sido tecleada, siendo una variante de este tipo de troyano el captapantalla o «*screenlogging*», técnica en la que la captura se realiza sobre imágenes de una pantalla que se remiten al atacante sin conocimiento del usuario del equipo[38]; una tercera modalidad es la de los ladrones o «*stealers*», que directamente acceden y roban información que se encuentre almacenada en el equipo y la envían a un atacante, pudiendo ser contraseñas, correos electrónicos o algún tipo de mensajería instantánea; en cuarto lugar, se hallan los secuestradores o «*ransomware*», a través de los cuales se puede bloquear y secuestrar el acceso a un equipo o a la información que este contiene, cifrándola, para des-

[37] *Ibídem,* pág. 234.
[38] *Ídem*, pág. 246.

pués pedir un rescate económico para desbloquearlo[39]; y, por último, un tipo de troyano especialmente empleado para el ciberespionaje es el evasor, conocido con el nombre de *virus duqu*, actualizado en su versión *Duqu 2.0.*, que no solo descarga archivos infectados en el ordenador, sino que además permite robar información de este, siendo su más destacada peculiaridad las sofisticadas técnicas de evasión que emplea, lo que hace especialmente difícil su detección[40].

2. Suplantadores de identidad (*Phishing*)

Esta modalidad de ciberataque constituía en un origen —como apunta González Cussac— una técnica de obtención de contraseñas para usurpar la identidad del legítimo titular de una cuenta y así apropiarse de su dinero en operaciones de banca electrónica. Sin embargo, posteriormente la finalidad defraudatoria no era la única que podría perseguirse[41]. Así empezó a emplearse esta modalidad para otros fines, como el de obtener información ajena, ya fuera de carácter personal o empresarial, lo cual se lograba a través del envío de un correo electrónico con apariencia de tener carácter oficial, empleándolo como cebo para dirigir al usuario a páginas falsas en las que le pedían información confidencial[42]. Una modalidad de los suplantadores de identidad que ha adquirido especial protagonismo como forma de ataque encuadrable en la interceptación de las telecomunicaciones son los suplantadores de identidad selectivos o «*spear phishing*», los cuales operan del mismo modo que lo hace la modalidad genérica, pero su peculiaridad reside en que, mientras esta última se dirige indistintamente a multitud de usuarios al azar, la selectiva escoge grupos determinados de personas con algo en común[43], que en el caso del delito de espionaje podría ser un grupo de empresas del mismo sector de mercado, empleados de una compañía concreta, o cualquier grupo de personas que compartan algún tipo de actividad profesional. El medio engañoso que

[39] INCIBE (Instituto Nacional de Ciberseguridad de España): «Descubre los diferentes tipos de malware que pueden afectar a tu pyme», publicado el 9 de mayo de 2016 (https://www.incibe.es/protege-tu-empresa/blog/descubre-tipos-malware).

[40] INFOSEC INSTITUTE: «Duqu 2.0.: The Most Sofisticated Malware Ever Seen», June 17, 2015. En este artículo se señala que víctima de amenaza mediante este tipo de troyano ha sido recientemente la empresa de seguridad Kaspersky Lab.

[41] GONZÁLEZ CUSSAC, J.L.: Tecnocrimen. *Op. cit*., pág. 216.

[42] Así lo pone de manifiesto el *Federal Bureau of Investigation (FBI)* de los Estados Unidos, en una publicación del 4 de enero de 2009 que llevaba por título «Spear Phishers: Angling to Steal Your Financial Info» (https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109)

[43] *Ibídem*.

emplea esta técnica es el envío de un correo electrónico procedente de una empresa familiar o alguien conocido, el cual contiene un enlace en el que presionan y donde se les solicita la provisión de información como contraseñas, números de cuenta, usuarios, códigos de acceso, etc.[44] Así, la finalidad que persiguen los suplantadores de identidad selectivos es la de obtener ilícitamente propiedad intelectual, datos financieros, secretos comerciales u otra información reservada.

3. Encubridores (*Rootkits*)

Estos constituyen otro tipo de programa malicioso que afecta especialmente a dispositivos móviles o a tabletas electrónicas, y que permiten un acceso privilegiado de forma continuada a dicho dispositivo pero oculto a sus administradores, lo cual lo hace especialmente difícil de descubrir. Este tipo de ataque, que no exige especiales conocimientos técnicos para ejecutarlo, pero que emplea métodos cada vez más sofisticados[45], permite al sujeto activo controlar el dispositivo, lo que incluye «apropiarse de todos los datos personales; interceptar y redirigir llamadas; utilizar el micrófono para realizar escuchas; grabar imágenes y vídeos desde la cámara; capturar las pulsaciones del teclado; localizar la ubicación de la víctima a través del GPS»[46], entre otras consecuencias. Cualquier videoconferencia que esté teniendo lugar o toda comunicación que se esté desarrollado en un chat privado puede ser objeto de ataque a través de esta vía.

4. Programas espías (*Spyware*)

Este constituye el medio de interceptación por excelencia para realizar un ciberataque. Son programas cuyo fin es el de recolectar información sobre la actividad de un usuario, ya sea un individuo o una empresa, para después enviarla a una entidad externa, dependiendo la cantidad de información con la que pueden hacerse del tiempo que pase sin ser detectados[47].

---

[44] *Ídem*; PATTERSON, T.: «Chinese cyber spies may be watching you, experts warn», en *CNN*, de 28 de agosto de 2016 (http://edition.cnn.com/2016/08/23/us/declassified-china-cyber-espionage/)

[45] MORÓN LERMA, E.: «Quiebras de la privacidad en escenarios digitales: Espionaje industrial», en *InDret*, núm. 21, 2007, pág. 127.

[46] GONZÁLEZ CUSSAC, J.L.: Tecnocrimen. *Op. cit*., pág. 217.

[47] INCIBE: Descubre los diferentes tipos de malware. *Op. cit*.

En definitiva, dadas las diversas formas de ataque que presenta el uso ilícito de las nuevas tecnologías de la información y la comunicación, se hace obligatoria una tipificación altamente especializada y precisa, que esté en constante transformación y evolución[48]. En este sentido, resulta necesaria una interpretación amplia *de lege lata* del término interceptación, que desatienda su sentido estrictamente gramatical, insuficiente por sí solo para determinar los contornos de esta forma de obtención ilícita de información.

IV. LA INTELIGENCIA COMPETITIVA COMO RIESGO DEL SIGLO XXI

La inteligencia, basada en el concepto de estrategia[49], consiste en encontrar y analizar información para actuar de forma estratégica, cualquiera que sea su ámbito y constituye el reverso de las distintas conductas de espionaje, surgiendo también para combatirlo ante las dificultades que su lucha presenta. Dichas dificultades se acrecientan ante la realidad actual en la que dos elementos marcan el rumbo de la actividad económica: la globalización de los mercados y el constante auge de las nuevas tecnologías. A los efectos que aquí interesan, aludiremos a tres tipos de inteligencia: la económica, la jurídica y la competitiva o empresarial.

En primer lugar, el concepto de *inteligencia económica*[50] puede entenderse como «el conjunto de acciones coordinadas de investi-

[48] GONZÁLEZ CUSSAC, J.L.: Tecnocrimen. *Op. cit*., pág. 225.

[49] Una explicación de los distintos tipos de inteligencia puede encontrarse en OLIER ARENAS, E.: «Inteligencia estratégica y seguridad económica», en *Cuadernos de Estrategia 162-La inteligencia económica en un mundo globalizado*, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2013, págs. 16-19.

[50] La inteligencia económica, que en España aún no ha tenido un fuerte anclaje a diferencia de lo que ocurre en otros países como Estados Unidos o Francia, se definió por la Ley francesa n.º 2011-267, de orientación y programación para la actuación de la seguridad nacional, de 14 de marzo de 2011, en su artículo 32, como la búsqueda y el tratamiento de informaciones sobre el entorno económico, social, comercial, industrial o financiero de una o más personas físicas o jurídicas, con el objetivo de permitir que se protejan de los riesgos que puedan amenazar su actividad económica, su patrimonio, sus activos inmateriales o su reputación, así como de favorecer su actividad. Sin embargo, esta disposición, entre otras, fue declarada inconstitucional por el Consejo Constitucional en Decisión n.º 2011-625 DC, de 10 de marzo de 2011, por la indefinición tanto de las actividades susceptibles de ser consideradas inteligencia económica, como de su objetivo (WARUSFEL, B. : «L'intelligence juridique, complément nécessaire de l'intelligence économique», en *Rue Saint Guillaume, n.º 162 (Dossier : À quoi sert l'intelligence économique ?*), mars-avril, 2011, págs. 26-27). Puede ahondarse en la citada Ley, así como en la declaración de inconstitucionalidad, en http://www.senat.fr/dossier-legislatif/pjl09-292.html

gación, tratamiento y distribución de la información para tomar decisiones en el orden económico»[51]. En esta actividad, en el ámbito español, el actor principal sería el Estado, con el fin de defender sus intereses económicos en el marco internacional[52]. El reverso de este tipo de actividad lícita sería el espionaje económico que tiene lugar entre Estados, del que serían buen ejemplo los casos de Rusia o China[53]. La alusión a este tipo de inteligencia resulta necesaria para no confundirla con la que aquí interesa, que es la empresarial o competitiva, y que podría englobarse dentro de la económica, cuando el actor de esta fuera el Estado[54].

En segundo lugar, la llamada *inteligencia jurídica* puede definirse como «el conjunto de técnicas y medios que permiten a un actor —privado o público— conocer el entorno jurídico en el que participa, para identificar y anticipar los riesgos y las oportunidades potenciales de actuación, (…) así como disponer de las informaciones y derechos necesarios para poder poner en práctica los instrumentos jurídicos aptos para realizar sus objetivos estratégicos»[55]. El conocimiento de este tipo de información permite a las empresas, como actores privados, garantizar la protección jurídica de sus bienes inmateriales, como son los secretos de empresa, desarrollando estrategias preventivas para ello.

En tercer lugar, crucial en el ámbito que estudiamos resulta la *inteligencia competitiva* o *empresarial*, para la cual los dos tipos de inteligencia apenas comentados resultan de especial relevancia. Este tipo de inteligencia consistiría en la búsqueda lícita y el análisis de información útil en términos competitivos para sacar provecho de ella y mejorar así la posición en el mercado, pudiendo esta ser realizada por el Estado o por las empresas[56]. Esta actividad constituye

---

[51] OLIER ARENAS, E.: Inteligencia estratégica. *Op. cit*., pág. 11.

[52] *Ibídem*, pág. 17.

[53] Afirman expertos en tecnologías emergentes que China se ha cansado de ser la fábrica del mundo y que sus actividades de ciberespionaje son parte de un gran esfuerzo por reducir su dependencia de tecnología extranjera, aspirando a cambiar el «*made in*» por el «*innovated in*» (SEGAL, A.: «Curbyng Chinese Cyber Espionage», en *Council on Foreign Relations (CFR)*, de 9 mayo de 2011 (http://www.cfr.org/cybersecurity/curbing-chinese-cyber-espionage/p24935).

[54] Dentro de esta, se ha hecho también una distinción entre inteligencia microeconómica y macroeconómica, incluyendo en la primera, entre otros aspectos, la defensa del valor e integridad de activos inmateriales de las empresas nacionales frente a ataques como el ciberespionaje, el robo de patentes, la piratería intelectual y en el diseño (ESTEVE MORA, F.: «La inteligencia económica», en *El País*, 25 de julio de 2013, pág. 2).

[55] WARUSFEL, B. : L'intelligence juridique. *Op. cit*., pág. 29.

[56] OLIER ARENAS, E.: Inteligencia estratégica. *Op. cit*., págs. 17-18.

una práctica cada vez más frecuente en la búsqueda de una posición óptima en el mercado y la doctrina anglosajona se ha hecho eco de ello, publicando técnicas o estrategias para adquirir información de los competidores por parte de las empresas[57]. También se ha puesto de manifiesto cómo la puesta en práctica de inteligencia competitiva ha creado un nuevo mercado para una clase emergente de empresas de espionaje privadas, creadas por veteranos de las agencias de inteligencia del mundo, como la CIA, que venden sus servicios por contrato a empresas y firmas financieras[58]. Todo lo anterior pone de manifiesto la relevancia de la inteligencia competitiva, siendo esta la que se ha desarrollado con mayor profundidad, por lo que en ella nos centraremos.

Como puede observarse, cada tipo de inteligencia puede concernir a diversos actores, pero su contenido difiere. Sin embargo, la inteligencia jurídica, como complemento necesario de la inteligencia económica[59], también lo es de la competitiva o empresarial, y esta última encuentra su límite en el espionaje empresarial, en general, y en el ciberespionaje, en particular. En este sentido, resulta clave tener presente que un requisito fundamental de la inteligencia competitiva es la *licitud* de sus medios de búsqueda en fuentes de acceso público[60], por lo que toda indagación de información empresarial de un competidor cuya obtención suponga vulnerar las barreras de lo legítimo, quedaría extramuros del concepto de inteligencia y pasaría a formar parte del espionaje empresarial. Así, existen ciertas vías lícitas de hacerse con información empresarial ajena, sin el consentimiento de su titular, siempre que sobre ella no recaiga un derecho absoluto de propiedad industrial. Entre ellas se encuentran la in-

[57] BAGNOLI, M. / WATTS, S.G.: «Competitive intelligence and disclosure», *The RAND Journal of Economics*, Vol. 46, No. 4 (winter 2015); SUBRAMANIAN, R. / ISHAK, S.T.: «Competitor Analysis Practices of US Companies: An Empirical Investigation», *MIR: Management International Review*, Vol. 38, No. 1 (1st Quarter, 1998); ZHENG, Z. / FADER, P. / PADMANABHAN, B.: «From Business Intelligence to Competitive Intelligence: Inferring Competitive Measures Using Augmented Site-Centric Data», *Information System Research,* Vol. 23, No. 3, Part 1 of 2 (september 2012).

[58] JAVERS, E.: «Secrets and Lies: Rise of Corporate Espionage in a Global Economy», Georgetown Journal of International Affairs, Vol. 12, No. 1 (Winter/ Spring 2011), págs. 56-58.

[59] WARUSFEL, B. : L'intelligence juridique. *Op. cit*., pág. 26.

[60] PALOP MARRO, F.: «La inteligencia para competir: nuevo paradigma en la dirección estratégica de las organizaciones en un mundo globalizado», en *Cuadernos de Estrategia 162-La inteligencia económica en un mundo globalizado*, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2013, pág. 144. Este autor afirma que, mientras que la inteligencia competitiva es ética, legal y legítima, el espionaje comercial es ilegal e innecesario.

geniería inversa, las investigaciones independientes y los descubrimientos por azar y todos ellos serían medios posibles en el contexto de la inteligencia competitiva.

Un supuesto interesante en este ámbito, por el carácter discutido que puede tener como conducta fronteriza entre la inteligencia competitiva y el espionaje empresarial, es el que plantea el llamado basureo o buceo de contenedores, más conocido con el término anglosajón de *dumpster diving*, que consiste en rebuscar información relevante en la basura que genera una empresa. Esto fue lo que ocurrió en el *caso Oracle vs. Microsoft*, en el que el primero contrató a una empresa de investigación para obtener información del segundo, utilizando para ello, entre otros medios, esta práctica.

Especial mención merecen actualmente en este contexto los llamados *metadatos*, pues la referencia a los datos en el tipo delictivo los incluye también como posible objeto de la conducta. Los metadatos son definidos como «datos sobre los datos» o como «descripciones de los datos»[61]. Un ejemplo claro puede venir dado con el título que damos a un documento electrónico cualquiera, ya sea privado o en el contexto de una empresa, el cual sería un dato del texto, a la vez que un metadato, pues estaría entre la información que describe el documento. Junto al título, otros metadatos de un documento electrónico pueden ser, por ejemplo, la fecha de su creación, la cuenta de usuario desde la que fue realizado o su dirección IP, su tamaño, su última modificación, el tiempo de edición o el equipo desde el que lo creó, entre otros. Estos metadatos, o datos sobre el documento, pueden aportar una valiosa información sobre el contenido de aquel, aun cuando no se acceda a este. Junto a este ejemplo, se pueden aportar otros, como los metadatos que se desprenden de una simple llamada telefónica o de un correo electrónico, pues si accedemos al registro de llamadas o a la bandeja de entrada podemos ver información como la hora, la fecha, el emisor o incluso la localización de una llamada o mensaje, y en este último caso también su asunto puede tener un importante valor[62]. Sin embargo, para que

[61] INSTITUTO GEOGRÁFICO NACIONAL DEL MINISTERIO DE FOMENTO: *Geoportal de metadatos de información geográfica* (http://metadatos.ign.es/web/guest/introduccion)

[62] Piénsese en el supuesto en el que una empresa textil se encuentra buscando nuevos proveedores, y su competidor accede a la bandeja de entrada de un correo corporativo, donde ve un mensaje de un importante proveedor de ropa, recibido el día en el que tenía que decidirse su contratación, cuyo asunto fuera «Acuerdo». No haría falta acceder al contenido de dicho mensaje para saber qué había ocurrido y qué decía, aun cuando posteriormente su contenido pudiera ser otro, se habría obtenido información valiosa para la empresa.

los metadatos puedan ser considerados secreto de empresa, y como ocurre con cualquier tipo de información, es necesario que su titular haya adoptado las medidas pertinentes para su protección, lo cual en el caso de este tipo de información es habitual que se descuide. Queda claro que en el supuesto de una cuenta de correo electrónico o de un teléfono, en la medida en que se establecen contraseñas de acceso y medidas de seguridad para proteger la información contenida en ellos, los metadatos reciben también dicha protección. Sin embargo, hay otros casos en los que se descuida por parte del titular la protección de esta información, como por ejemplo, cuando se publican ciertos documentos para su descarga en la web de la empresa, sin que se suprima previamente la información añadida sobre dicho documento.

En estos casos, si un competidor extrae información de los metadatos de esos archivos, queda patente que su titular no puede ampararse en que dicha información constituye secreto de empresa, al haberla hecho pública él mismo. Lo mismo puede decirse de los casos citados previamente referidos al basureo, si pensamos en el basureo digital, como es el caso cuando se eliminan archivos y se envían a la papelera del ordenador. En ambos supuestos, atendiendo al bien jurídico protegido no existiría ya objeto alguno de propiedad pues, si bien puede imaginarse el caso en que la persona que ha desechado dicha información se arrepienta y vuelva a buscarla antes de que definitivamente salga de su esfera de control, el haberlo hecho supone la desprotección de la información como valor empresarial[63], por lo que no existiendo ya bien inmaterial objeto de la propiedad, no habría acceso ilícito ni tampoco ataque penalmente reprochable. A mi juicio, estos comportamientos solo podrían dar lugar en todo caso a actos desleales contrarios a la buena fe comercial, sancionables por la vía del artículo 4.1 LCD[64].

Por todo ello, como apunta Vilas Rodríguez, resulta de vital importancia para minimizar riesgos, implantar medidas que protejan la información sensible, tanto mientras está almacenada, como

[63] Comparemos el secreto de empresa con un gas que se pretende conservar. Para ello, un sujeto debe ineludiblemente introducirlo en un bote de cristal, pues de lo contrario no tendrá nada que conservar, en la medida en que se esfumará en el aire. Si el sujeto llegara a romper el bote de cristal o a abrirlo, habrá perdido el gas. Algo similar ocurre cuando se desechan los secretos a la basura, afectando así a su propia existencia.

[64] Respecto de esta práctica en el ámbito civil, ESTRADA I CUADRAS, A.: *Violaciones de secreto empresarial. Un estudio de los ilícitos mercantiles y penales*, Atelier, Barcelona, 2016, pág. 59, señala que en la jurisprudencia jurídico privada estadounidense, la balanza se estaría decantando hacia el lado de la desaprobación.

cuando está en tránsito[65], pues en el momento en el que se abandonan las medidas de protección del secreto, este pierde su existencia misma, por lo que no resultaría esta una práctica penalmente reprobable y, por tanto, podría llegar a constituir un medio de inteligencia competitiva.

Teniendo esto en cuenta, autores estadounidenses han afirmado que la propia Ley contra secretos de empresa de este país («*Economic Espionage Act*») mejora la práctica de la inteligencia competitiva y sus técnicas, al poner de relieve la ilegitimidad de los medios reprobables que el espionaje empresarial emplea[66]. Dichos medios reprobables vienen dados, como se ha visto, por un acceso ilícito en la esfera privada de la empresa donde se encuentra la información, para lo cual es necesaria la superación ilícita de las barreras impuestas por su titular para protegerla.

Lo anterior pone el acento en la importancia de la protección de los secretos por parte del titular de la información de su empresa, no solo por ser clave para distinguir la inteligencia competitiva del espionaje empresarial, sino para que el propio empresario evite exponer al público su información relevante en un contexto en el que tiende a imperar la cultura de la inteligencia competitiva[67], y en el que los riesgos para la seguridad de la información son cada vez mayores ante la presencia de las sofisticadas técnicas de ataque que ofrecen las nuevas tecnologías.

Sin embargo, la importancia de la protección de la información empresarial ante los crecientes peligros que la acechan no puede hacernos perder de vista que dichas amenazas constituyen apriorísticamente un riesgo para la propiedad de los bienes inmateriales de su legítimo titular, encarnados por el secreto de una empresa, pero no un peligro de índole estatal, que pone en jaque la seguridad na-

[65] VILAS RODRÍGUEZ, J.: «La contrainteligencia en el sector de la industria», *Economía Industrial*, n.º 405, 2017 (ejemplar dedicado a: Nuevas tecnologías digitales), pág. 137. Este autor afirma que, para proteger la información en ambos formatos es de gran utilidad el empleo de sistemas criptográficos, pues estos garantizan tanto la confidencialidad (a través de su cifrado), como la integridad de la información (protección con firmas digitales).

[66] HOROWITZ, R.: «Competitive Intelligence, Law, and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time)», en *Strategic and Competitive Intelligence Professionals (SCIP)*, volume 14-number 3, july-september, 2011, pág. 43.

[67] GONZÁLEZ CUSSAC, J.L.: Tecnocrimen. *Op. cit*., pág. 238, ha señalado que el crecimiento de la cibercriminalidad no obedece solo a insuficiencias legales al definir los ilícitos, al establecer los procedimientos procesales o al regular la cooperación de las agencias de seguridad, sino que en gran medida dicho crecimiento es también imputable a la negligencia de las personas.

cional, a menos que se den circunstancias que repercutan de forma importante en infraestructuras críticas o que detrás de los ataques se encuentren otros Estados, haciendo de la cuestión un problema nacional. Esta última aclaración responde a la reciente posición de un sector doctrinal que, abogando por la creación de una suerte de macro-concepto de seguridad que se identifique con la de carácter nacional, comprenda dentro de él cualquier tipo de seguridad, donde se incluye la del comercio y, como ataque a esta, el espionaje o los ataques cibernéticos[68]. Hasta qué punto debe intervenir el Estado para defender los intereses de las empresas es una cuestión polémica[69] y esta tiene un especial protagonismo en Estados Unidos[70], donde la Ley contra el espionaje económico en beneficio de empresas privadas, que entró en vigor en enero de 2014, permitía dicha actividad solo para proteger la seguridad nacional de los Estados Unidos y de sus socios y aliados, pero no así para proporcionar una ventaja competitiva a las empresas y los sectores comerciales estadounidenses[71]. Sin embargo, no es este el lugar para ahondar sobre esta cuestión, lo que precisaría una mayor reflexión.

[68] En este sentido, GONZÁLEZ CUSSAC, J.L.: «Inteligencia jurídica: el valor estratégico del derecho en la seguridad económica», en *Cuadernos de Estrategia 162-La inteligencia económica en un mundo globalizado*, págs. 103-133, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2013, págs. 114-115; LARRIBA HINOJAR, B.: Ciberespionaje económico. *Op. cit*., págs. 333-334, quien señala que desde el año 2011 los Estados toman más conciencia de la amenaza real que supone el ciberespionaje económico para la seguridad nacional, al provocar este, no solo pérdidas económicas inmediatas, sino la destrucción de la ventaja competitiva de un país. Desde esta perspectiva, según la autora, la seguridad nacional ya no sería considerada solo desde una perspectiva exclusivamente militar y asociada a la defensa, sino también respecto de la seguridad en el ámbito económico.

[69] Los medios de comunicación, como no podía ser de otra forma, se han hecho eco de esta cuestión, entrevistando a expertos en la materia que han afirmado que el desarrollo de la inteligencia depende de las empresas, pero que estas cuentan con apoyo del gobierno. De este modo, competencia de las primeras sería, mediante el análisis de inteligencia, descubrir canales de comercialización, conocer las fortalezas y debilidades de sus competidores, las necesidades de sus clientes, entre otras cuestiones estrictamente comerciales; mientras que el gobierno se ocuparía más bien de otros aspectos relacionados con los negocios, pero que tengan que ver con la injerencia política, la inseguridad jurídica o la corrupción (GUALDONI, F.: «La hora de la inteligencia económica», en *El País*, 26 de octubre de 2014).

[70] WALKER, M.: «Should Intelligence Support to Private Industry Enhanced?», *Georgetown Journal of International Affairs*, Vol. 12, No. 1 (winter/spring 2011).

[71] RASCOFF, S.J.: «The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections», *The University of Chicago Law Review*, Vol. 83, No. 1 (winter 2016), pág. 252. Especialmente interesante resulta la evolución de esta norma, expuesta por este autor (págs. 252-258).

V. FINALIDADES DEL CIBERESPIONAJE DE EMPRESA

El tipo del artículo 278.1 CP prevé expresamente la concurrencia de un elemento subjetivo, que exige que la conducta tenga lugar «para descubrir un secreto de empresa»[72]. Sin embargo, además de los pormenores del elemento subjetivo del ciberespionaje *per se*, las conductas de acceso ilícito a sistemas de información ajenos pueden tener diversos objetivos posteriores, siendo el más común de ellos el aprovechamiento de la información para obtener algún tipo de beneficio propio o a través de su revelación a un tercero. No obstante, junto con dicha finalidad pueden darse otras que no constituirían espionaje propiamente dicho, pero que acompañan a los objetivos de utilizar o revelar, como puede ser la de destruir la información para generar un perjuicio a la empresa víctima del ataque. A continuación, pondremos de relieve las peculiaridades de cada uno de ellos y cuál es la vía para castigarlos en España.

A. La revelación de la información obtenida mediante ciberespionaje

El ciberespionaje constituye una de las modalidades comisivas del tipo de espionaje empresarial del artículo 278.1 CP. Sin embargo, el mismo precepto en su apartado segundo recoge una agravación de las consecuencias punitivas del espionaje, castigando al sujeto activo de este delito con la misma pena de multa, de doce a veinticuatro meses, y con prisión de tres a cinco años «…si se difundieren, revelaren o cedieren a terceros los secretos descubiertos».

La previsión por el legislador penal de los verbos típicos de difundir, revelar y ceder, derivada del traslado acrítico que este hizo de los delitos relativos a la intimidad (artículo 197.1 CP) para la tipificación del espionaje empresarial, responde a la voluntad de intentar abarcar todo tipo de comunicación de la información, desde la que se da a un solo sujeto (revelación y cesión) hasta aquella otra en la que esta se convierte en pública y notoria (difusión). De este modo, cabría concluir que en realidad la difusión no es más que una revelación o cesión realizada a un gran número de destinatarios. Sin embargo, a mi juicio, el empleo de los tres verbos resulta reiterativo e innecesario, pues en todo caso el número de personas a las que se

[72] Para mayor detalle sobre este elemento subjetivo del tipo y sus diferentes interpretaciones, *cfr*. FERNÁNDEZ DÍAZ, C.R.: «La finalidad de descubrir un secreto de empresa en el delito de espionaje empresarial», *Revista General de Derecho Penal*, 26 (2016).

comunique el secreto empresarial resulta irrelevante a efectos de entender cometido el delito del artículo 278.2 CP, ya que la pena a la que da lugar su comisión es la misma[73]. Por ello, se estima, con la opinión mayoritaria, que en definitiva los tres son términos equivalentes[74], y que habría bastado con emplear uno solo, como ya apuntara Morón Lerma[75] y como hacían el Proyecto de Código penal de 1992 (artículos 284 y 285) y el Anteproyecto de 1994 (artículos 273 y 274), que solo contemplaban la acción de «revelar»[76]. El medio comisivo de la revelación resulta indiferente, pudiendo llevarse a cabo de cualquier forma[77], aunque el tipo no lo diga expresamente.

El desvalor de resultado de todas las conductas incluidas en el art. 278.2 radica en hacer que una o varias personas ajenas a la información empresarial reservada la tengan bajo su dominio, pudiendo disponer de ella. De este modo el núcleo de lo injusto reside en la

[73] Critica esta solución CARRASCO ANDRINO, M.ªM.: *La protección Penal del Secreto de Empresa*, Cedecs Editorial, Barcelona, 1998, pág. 206, apuntando que una vez que la información secreta se convierte en notoria, «desaparece el interés económico ligado a esta situación, al pasar a ser de libre disposición el conocimiento antes reservado». Por ello, la autora estima que podría haberse castigado con mayor pena al que realiza una difusión generalizada de la información empresarial reservada.

[74] BAJO FERNÁNDEZ, M. / BACIGALUPO SAGGESE, S.: Derecho penal económico, 2.ª ed., Editorial Universitaria Ramón Areces, Madrid, 2010, pág. 543, quienes afirman que «por difundir, revelar o ceder debemos entender lo mismo que divulgar, lo que equivale a la comunicación a una o más personas no poseedoras del secreto, siendo indiferente que se comunique a una o más personas, por lo que la divulgación no exige que los secretos se conviertan por ello en notorio»; CARBONELL MATEU, J.C. / GONZÁLEZ CUSSAC, J.L.: Título X. Delitos contra la intimidad. *Op. cit*., págs. 1002 y 1007, quien equipara dichos términos al de «divulgación»; MORÓN LERMA, E.: La tutela penal del secreto de empresa. *Op. cit.,* pág. 629, quien señala que, *de lege lata*, todos los términos son equivalentes, pero que *de lege ferenda*, debería emplearse un único término.

[75] MORÓN LERMA, E.: *Ibídem,* pág. 628.

[76] *Ídem,* pág. 628, quien señala que, junto a otros términos posibles *de lege ferenda*, podrían proponerse otros como el previsto en el artículo 13.1 de la Ley de Competencia Desleal o en el artículo 39.2 del Acuerdo ADPIC, que aluden a «divulgar» o el que prevé la normativa alemana, cuyo §17 UWG se refiere a la «comunicación».

[77] MARTÍNEZ-BUJÁN PÉREZ, C.: *Delitos relativos al secreto de empresa*, Tirant Lo Blanch, Valencia, 2010, pág. 62 nota 108; MORÓN LERMA, E.: *Ídem,* pág. 626; PÉREZ DEL VALLE, C.: «La revelación de secretos de empresa por persona obligada a reserva (art. 279 CP)», *Cuadernos de Derecho* Judicial, n.º14, 1997, págs. 112-113, quien afirma que «…es irrelevante que el autor haya transmitido los datos con la entrega de papeles, documentos, informes, planos o cálculos escritos o de soportes de sonido (cintas de cassette o magnetofónicas) e informáticos (diskettes, CD's) que contienen esos datos; o lo haya hecho a través de la comunicación verbal directa o a través de medios de comunicación telefónica o electrónica (correo electrónico)».

pérdida de control sobre la información y su potencial explotación o nueva divulgación, pues con ello el titular pierde su exclusividad.

De esta forma, podría decirse que son dos los *efectos formales* que pueden tener lugar en virtud de la conducta realizada: por un lado, si la comunicación se produce a una pluralidad de personas, la información pasaría a ser notoria, perdiendo así su carácter secreto; por otro lado, si se hace a una sola persona o varias, quizás no se convierta en notoria, pero puede igualmente ser susceptible de perder el valor que ostentaba por tener carácter reservado, acabando así con su exclusividad. Con ello, dada la naturaleza vulnerable de la información y el valor relativo para la empresa que la posee, derivado de su carácter reservado, su mera comunicación a un sujeto concreto, aun cuando no la convierta en notoria, produce una pérdida potencial de su valor. Por tanto, no es preciso que la información se convierta en notoria para que se dé el *efecto material* que pretende evitarse con el presente delito y que radica en una pérdida del valor de la información a que da lugar su carácter secreto, bastando solo con la comunicación a una única persona para que ello se produzca.

B. La utilización de la información obtenida mediante ciberespionaje

Definido ya el ámbito típico de la revelación como toda puesta bajo el dominio o control de un tercero de información empresarial reservada que no debería conocer, queda claro que el desvalor de acción de este comportamiento difiere del de la conducta de utilización de secretos de empresa. Esta última debe ser entendida como sinónimo de explotación o de aprovechamiento. Según una interpretación teleológica de la conducta de «utilización» referida a secretos de empresa, por tal debe entenderse *toda actuación guiada por el contenido de dicha información*[78], independientemente de que esta llegue o no al conocimiento de terceros.

Dicha concepción del término abarcaría cualquier explotación del secreto de empresa derivada de su ejecución o puesta en práctica en un ámbito de negocio (*supuestos de aprovechamiento activo*)[79]

[78] En este sentido, PRIETO DEL PINO, A.M.: *El Derecho Penal ante el uso de información privilegiada en el Mercado de Valores*, Thomson Aranzadi, Navarra, 2004, pág. 346, respecto del delito de uso de información privilegiada en el mercado de valores.

[79] Así, este puede tener lugar, entre otras formas posibles, según el tipo de información en cuestión, mediante su aplicación a la producción de la empresa (si se trata generalmente de un secreto industrial, por ejemplo, de una fórmula o una idea

o bien del aprovechamiento de su conocimiento para conseguir una ventaja omitiendo una actuación en un determinado sentido, si se trata de una información negativa que permite dar a conocer vías de actuación fallidas[80] (*supuestos de aprovechamiento omisivo*)[81]. La aceptación de estos últimos casos puede plantear mayores dificultades, si pretende entenderse la utilización como una conducta exclusivamente activa. Sin embargo, su admisión es perfectamente posible, pudiendo apreciarse que se da un comportamiento activo u omisivo de aprovechamiento del secreto empresarial, cuando existe un *nexo intelectual* entre el conocimiento del contenido de este y la conducta del sujeto activo[82].

La previsión de ambas conductas, revelación y utilización, en los textos legales suele aparecer diferenciada pero en un mismo precepto, acogiendo así las dos finalidades que puede tener el ciberespionaje empresarial. En primer lugar, la normativa extrapenal vigente, plasmada en el artículo 13.1 de la Ley de Competencia Desleal los prevé aludiendo a la «divulgación» y «explotación»[83], afirmando sin embargo la doctrina mercantil que el hecho de que el destinatario receptor del secreto empresarial no llegue a explotarlo o que no pueda obtener ningún provecho de él, no son circunstancias que se

---

sobre sus productos) o mediante su recurso para actuar en el ámbito de los negocios (si se trata de secretos comerciales, por ejemplo, comercialización de determinados productos, información sobre sus proveedores o sobre sus clientes: productos adquiridos, franjas horarias de mayor número de ventas, etc.).

[80] Este tipo de información en Estados Unidos está dotada de una protección limitada. Así, mientras la *Economic Espionage Act* de 1996, de carácter federal, la excluye de su tutela, la *Uniform Trade Secrets Act* de 1985, de índole estatal, sí le ofrece protección (SIMON, S.: «The Economic Espionage of 1996», *Berkeley Technology Law Journal*, Vol. 13, No. 1, Annual Review of Law and Technology (1998), págs. 315-316).

[81] ESTRADA I CUADRAS, A.: Violaciones de secreto empresarial. *Op. cit.*, pág. 116; SUÑOL LUCEA, A.: *El Secreto Empresarial. Un Estudio del Artículo 13 de la Ley de Competencia Desleal*, Thomson Reuters, Civitas, Pamplona, 2009, págs. 289-290, quien afirma que el más claro ejemplo es el de la información negativa, y que su indirecto aprovechamiento en forma de ahorro de costes constituye una utilización a los efectos del artículo 13 LCD.

[82] PRIETO DEL PINO, A.M.: El Derecho Penal ante el uso de información privilegiada. *Op. cit.*, pág. 355, quien pone de manifiesto en relación con el delito de iniciados, que existirá «un *nexo intelectual* entre la información privilegiada y la operación realizada cuando la orden de negociación que hace posible la adquisición o cesión de valores haya sido elaborada mientras el sujeto estaba en posesión de dicha información».

[83] Dicho precepto establece que «se considera desleal la **divulgación o explotación**, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14».

exijan para que la divulgación se produzca[84]. En segundo lugar, la Directiva (UE) 2016/943 también los recoge conjuntamente en su artículo 4.3, refiriéndose a la «utilización» y a la «revelación»[85]. En tercer lugar, también otros ordenamientos aluden a ellas de manera conjunta, como es el caso del artículo 623 del Código penal italiano[86] o del § 17.2 *Unlautere Wettbewerb Gesetz* en el ordenamiento jurídico alemán[87]. Sin embargo, el legislador penal español ha tipificado la utilización de secretos de empresa solo en dos supuestos: en el delito especial del artículo 279.2 CP, es decir, para el sujeto con un deber legal o contractual de guardar reserva; y en el artículo 280, para quien realiza alguna de las conductas de los artículos anteriores y, por tanto, entre otras, la apenas citada, pero sin participar en su descubrimiento. Por el contrario, en el caso del espía de empresa el legislador penal no ha previsto dicha conducta que, constituyendo el agotamiento del presente delito, intensifica aún más la lesión del bien jurídico protegido.

Esta ausencia da lugar a soluciones penológica y político-criminalmente cuestionables, pues a quien personalmente se apoderare de forma ilegítima de un secreto de empresa, que posteriormente revela a un competidor, le es aplicable una pena de prisión de tres a cinco años; mientras que, si en lugar de revelarlo, él mismo es competidor directo del titular del secreto y lo explota, aprovechándolo

---

[84] SUÑOL LUCEA, A.: El Secreto Empresarial. *Op. cit.*, pág. 287.

[85] Así, la Directiva establece que «la **utilización o revelación** de un secreto comercial se considerarán ilícitas cuando las lleve a cabo, sin el consentimiento de su poseedor, una persona respecto de la que conste que concurre alguna de las condiciones siguientes:

—Haber obtenido el secreto comercial de forma ilícita;
—Incumplir un acuerdo de confidencialidad o cualquier otra obligación de no revelar el secreto comercial;
—Incumplir una obligación contractual o de cualquier otra índole de limitar la utilización del secreto comercial».

[86] El precepto italiano reza como sigue «Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, *le rivela o le impiega* a proprio o altrui profitto, è punito con la reclusione fino a due anni». La previsión conjunta aquí lleva a la doctrina a preguntarse si estamos ante un tipo mixto alternativo o acumulativo (así, GIAVAZZI, S.: *La tutela penale del segreto industriale*, Giuffrè Editore, Milano, 2012, págs. 351 y ss.).

[87] El precepto alemán prevé incluso el apoderamiento en el mismo precepto, estableciendo lo siguiente «Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, (...) ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlang oder sich sonst unbefugt verschafft oder *gesichert hat, unbefugt verwertet oder jemandem mitteilt*».

para obtener una ventaja ilegítima frente a aquel, solo sería castigado por el delito de apoderamiento, cuya pena es de dos a cuatro años de prisión[88]. Esto constituye una muestra de que lo que el legislador ha querido proteger es que no existan sujetos no autorizados que conozcan secretos de empresa ajenos. No obstante, una posible explotación por estos sujetos y, por tanto, intensificación de la lesión del bien jurídico, no debería quedar impune.

Sin embargo, esta laguna legal no resulta subsanable *de lege lata*, en aras del respeto al principio de legalidad, por ninguna de las otras dos vías donde dicha conducta se castiga de forma expresa en el Código por exigirse unos requisitos especiales al sujeto activo de cada uno de ellos[89].

Como una posible causa de esta ausencia podría pensarse que, dado que estamos ante un delito patrimonial, el legislador ha obviado el uso del secreto, como hace respecto del resto de delitos de esta naturaleza, con la salvedad del hurto de uso de vehículos. No obstante, la razón político-criminal por la que estas conductas suelen ser atípicas se fundamenta en la devolución de la cosa en un periodo de tiempo determinado, ya que la naturaleza material de esta lo hace posible. Ello no puede predicarse, en cambio, del bien sobre el que recae la conducta en el delito de espionaje, pues su carácter inmaterial hace que una vez sustraído de forma ilegítima por un sujeto ajeno a él, deje siempre la duda de si este sigue teniendo copias, a pesar de que asegure su devolución o destrucción. Esta es una razón más que fundamenta la necesidad del castigo de dicha conducta en este delito.

Sin embargo, a mi juicio, la citada ausencia no responde a este motivo, sino más bien a la cuestionable técnica legislativa empleada en el Código penal de 1995, según la cual los tipos de referencia a partir de los cuales se tipificó el espionaje empresarial fueron los delitos contra la intimidad, lo cual explica el paralelismo entre ambos grupos de delitos, ya puesto de manifiesto por la doctrina[90]. Este

[88] Así ocurrió, por ejemplo, en la SAP Zaragoza (Sección 3.ª), 259/2008, de 18 de abril, en la que un sujeto se apoderó de numerosa información de la anterior empresa para la que trabajaba, con accesos continuados mediante un uso ilegítimo de las claves que poseía entonces. A partir de la información obtenida, creó su propia empresa sin que llegara a revelar ninguna información.

[89] En el caso del artículo 279.2 CP, debe ser quien tuviere legal o contractualmente la obligación de guardar reserva y el del artículo 280 CP, quien realice las conductas previstas en los dos artículos anteriores, siempre que el sujeto activo no haya participado en el descubrimiento del secreto ni que conozca su origen ilícito.

[90] CARRASCO ANDRINO, M.M.: La Protección Penal del Secreto. *Op. cit.*, pág. 205; MORÓN LERMA, E.: La tutela penal del secreto de empresa. *Op. cit.*, págs. 617-618.

puede verse no solo en la reproducción prácticamente idéntica de las estructuras típicas, sino también en la remisión directa del artículo 278 CP al 197.1, en la redacción de las mismas conductas típicas, aun cuando no siempre tengan sentido en este contexto, en relación al elemento subjetivo del tipo o incluso en las penas a imponer, siempre superiores en el caso del espionaje empresarial[91].

Sin embargo, resulta necesario *vincular el tipo de secreto en cuestión al bien jurídico protegido* y ello lleva a que la protección conferida a un secreto relativo a la intimidad no pueda ser la misma que la que se prevé para el de empresa. De esta forma, siendo el bien jurídico protegido en el delito de espionaje empresarial la propiedad sobre un bien inmaterial, el secreto empresarial, el elemento clave no solo viene dado por la confidencialidad de la información, como ocurre en los delitos relativos a la intimidad, sino también, y sobre todo, por la *exclusividad en la facultad de su aprovechamiento económico*. Es la persecución de ese propósito lo que motiva a su titular a mantener en secreto la información, debiendo ser tenido en cuenta en la tipificación de las conductas.

Por ello, parece necesario otorgar a esta conducta una mayor relevancia en el ámbito del espionaje empresarial respecto de la que posee en los tipos de referencia a los que acudió el legislador para su tipificación, siendo precisa su introducción *de lege ferenda*.

C. La destrucción de la información empresarial ajena como fin complementario del ciberespionaje

La información empresarial de la que es objeto el ciberespionaje se caracteriza por su naturaleza inmaterial y ubicua, lo que hace que las formas de ataque a aquella difieran respecto de las que se pueden dar contra bienes materiales.

Así, mientras que el delito de espionaje, en general, y ciberespionaje, en particular, tiene como fin preservar la confidencialidad de la información empresarial ajena; los delitos de daños castigan con-

[91] En relación a las penas de prisión, el legislador simplemente aumentó los límites mínimos de los marcos penales del espionaje empresarial respecto a los de la intimidad. Así, el artículo 197.1 prevé una pena de prisión de uno a cuatro años, mientras que el 278.1 la establece de dos a cuatro años y el artículo 197.3 impone una pena de prisión de dos a cinco años, mientras que el 278.2 recoge una de tres a cinco años. En cuanto a las penas de multa, el artículo 278.1 mantiene inalterada la prevista en el 197.1 de doce a veinticuatro meses, mientras que el artículo 197.3 CP no prevé multa alguna, que sin embargo el legislador ha decidido imponer en el 278.2 CP, reproduciendo la misma que establece el párrafo primero.

ductas 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[92]. Estos últimos están previstos en los artículos 264 y 264 bis CP, donde se recogen los delitos de daños o sabotaje de datos y de sistemas informáticos.

Sin embargo, cabe una tercera posibilidad, derivada del carácter inmaterial de la información objeto de ataque y es que este puede producirse contra esos tres elementos simultáneamente: integridad, disponibilidad y confidencialidad[93].

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 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[94].

---

[92] 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 (HERRERA MORENO, M.: «Lección 8.ª. Daños», en POLAINO NAVARRETE, M. (dir.): *Lecciones de Derecho penal. Parte especial*, Tecnos, Madrid, 2011, pág. 133).

[93] INCIBE (Instituto Nacional de Ciberseguridad de España): «Guía de almacenamiento seguro de la información», 2016, pág. 5. En este sentido también, MORÓN LERMA, E.: Quiebras de la privacidad. *Op. cit*., pág. 130; RIBAGORDA GARNACHO, A.: «Seguridad de las tecnologías de la información», en *Ámbito jurídico de las tecnologías de la información,* CDJ, CGPJ, 1996*,* págs. 312-313, quien estima que un sistema es fiable cuando se satisfacen dichos elementos en los recursos que lo integran.

[94] En el mismo sentido, GUTIÉRREZ FRANCÉS, M.L.: «Delincuencia económica e informática en el nuevo código penal», en GALLARDO ORTIZ, M.A.: *Ámbito jurídico de las tecnologías de la información*, Consejo General del Poder Judicial, Madrid, 1996, pág. 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, C.: Delitos relativos al secreto*. Op. cit.,* pág. 56; MORALES PRATS, F.: Título X. Delitos contra la intimidad. *Op. cit.,* págs. 411-412; MORÓN LERMA, E.: La tutela penal del secreto de empresa. *Op. cit.,* pág. 853; PRATS, J.M.: «Descubrimiento y revelación de secretos de empresa en el Código penal de 1995», en DEL ROSAL BLASCO, B.: *Delitos relativos a la Propiedad Industrial, al Mercado y a los Consumidores*, CGPJ, Madrid, 1997, pág. 193.

Así, la sustracción de la información empresarial ajena 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 (como ocurrió, por ejemplo, en la SAP Tarragona —Sección 2.ª—, 4.4.2003); 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[95] (algunos ejemplos son la SAP Madrid —Sección 6.ª—, 345/2013, de 3 de junio y la SAN —Sala de lo Penal, Sección 4.ª—, 17/2015, de 11 de junio).

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 objeto de ataque. Dicho carácter hace que el ciberespionaje no implique siempre una desposesión y, por tanto, la pérdida definitiva de la información por parte de su titular[96]. Así, será habitual que el secreto se sustraiga sin levantar sospechas y conviva bajo el dominio de ambos sujetos, activo y pasivo. Sin embargo, en los casos en los que dicha desposesión se produce porque, además de hacerse con ella el autor del ciberataque, la destruye, estaremos ante supuestos en los que concurren los dos tipos subjetivos mencionados y en los que, por tanto, cabe aplicar un concurso ideal o real de delitos. Algunos ejemplos de este tercer caso de supuestos pueden encontrarse en el AAP Barcelona (Sección 2.ª), 18.7.2012, la SJP Terrassa (Sección 1.ª), 1.2.2006 y la SAP Sevilla (Sección 7.ª), 30.12.2011, entre otras muchas resoluciones.

[95] En este sentido también, CORCOY BIDASOLO, M.: CORCOY BIDASOLO, M.: «Capítulo IX. De los daños», en CORCOY BIDASOLO, M. / MIR PUIG, S. (dirs.): *Comentarios al Código penal. Reforma LO 5/2010,* Tirant lo Blanch, Valencia, 2011, pág. 586. Un sector doctrinal incluye, sin embargo, como posible intención del espionaje la destrucción del secreto. En este sentido se pronuncian, ESTRADA I CUADRAS, A.: Violaciones de secreto empresarial. *Op. cit*., pág. 65; MORÓN LERMA, E.: *El secreto de empresa. Protección penal y retos que plantea ante las nuevas tecnologías*, Aranzadi, Pamplona 2002, pág. 307, nota 27.

[96] Como apunta CASTRO MORENO, A.: Espionaje industrial y secreto de empresa. *Op. cit*., pág. 49, este sí sería el significado del verbo típico «apoderarse» en los delitos patrimoniales generales, donde se exige necesariamente la incorporación al propio patrimonio del sujeto del objeto en cuestión. Igualmente, el AAP La Rioja 148/2001, de 23 de octubre, señala que un posible apoderamiento de datos no necesita desplazar su soporte, o como mínimo no exige sacarlo de la esfera de dominio del titular.

VI. CONCLUSIONES

El auge de las nuevas tecnologías de la información y la comunicación ha facilitado la vida de los ciudadanos en numerosos ámbitos, a la par que ha creado nuevos medios de ofensa a bienes jurídicos de aquellos. Un buen ejemplo de ello es el que tiene lugar en el ámbito empresarial con las conductas de ciberespionaje. Estas irrumpen en el mercado, desestabilizándolo, mediante injerencias ilícitas en el capital inmaterial más vulnerable de las empresas, el que constituyen sus secretos.

En nuestro país estas conductas se producen con bastante frecuencia, a pesar de que se desconoce la cifra real de las mismas por la propia naturaleza del objeto inmaterial sobre el que aquellas recaen, ya que no siempre se sustrae a su titular definitivamente la información y que además es susceptible de perder todo su valor por la confidencialidad sobre la que su propia existencia se construye. Del estudio de la jurisprudencia se detectan casos que ponen de relieve la importancia del problema y de la lectura de los tipos penales que se encargan de su punición, las falencias que estos presentan.

En primer lugar, este precepto recoge un delito común que exige al sujeto activo un acceso ilícito, dejando fuera del tipo a todo aquel que conociera ya el secreto con el consentimiento de su titular, supuesto que entraría a formar parte del delito especial previsto en el artículo 279 CP, a pesar de que nuestros tribunales no siempre lo han entendido así.

En segundo lugar, la alusión a secretos de empresa exige una concreción de qué se entiende por tales, al no constituir propiamente categorías pertenecientes a la propiedad industrial en sentido estricto, por lo que, debido a esto último, no es posible su registro. Ello lleva a que su configuración parta de la ineludible adopción de medidas de protección de su reserva por su titular, sin las cuales no estaríamos ante un delito de ciberespionaje. El propio medio comisivo de acceso ilícito telemático ya denota una vulneración de medidas, sin embargo, la existencia de estas es clave en casos limítrofes como el basureo digital o la técnica de la inteligencia competitiva aplicada, sobre todo, a metadatos, casos en los que el descuido de aquellas convierte cualquier conducta en atípica.

En tercer lugar, la conducta típica de interceptación es la que castiga el ciberespionaje y debe ser interpretada de forma lo suficientemente amplia como para abarcar todas las modalidades comisivas posibles, que constantemente evolucionan. La referencia a las

telecomunicaciones, cuya definición por el Diccionario de la Lengua Española ha cambiado recientemente, se entiende adecuada para abarcar todos los soportes que contienen información digitalizada que pueda ser objeto de ciberespionaje.

En cuarto lugar, respecto a las conductas posteriores a las que puede dirigirse el ciberespionaje como finalidades del mismo, de forma correcta el tipo castiga la revelación de la información obtenida a través de aquel. Sin embargo, existe una importante laguna de punibilidad cuando, tras la obtención ilegítima de información ajena, esta es aprovechada económicamente sin revelación alguna. En estos casos, nuestro Código penal no ofrece una protección adecuada a la propiedad inmaterial de la empresa, siendo necesario el castigo de esta conducta *de lege ferenda*. Por lo que respecta a la destrucción de la información, la compatibilidad de ambos ataques contra la información hace que con frecuencia se presenten concursos entre el ciberespionaje y el delito de sabotaje informático, que no siempre se resuelven de la misma manera en nuestros tribunales.

En definitiva, puede decirse que, si bien el Código penal español ofrece una tutela que permite cubrir las modalidades comisivas del delito de ciberespionaje, cuyo mayor reto es su cada vez mayor sofisticación, existen todavía algunas aristas que precisan atención por parte del legislador y de la jurisprudencia. Y que, dada la frecuencia de su comisión y su, cada vez mayor, complejidad, su abordaje por el Derecho penal constituye todo un desafío del siglo XXI en España.

VII. BIBLIOGRAFÍA

ANARTE BORRALLO, E.: «Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código Penal», en *Jueces para la Democracia*, n.º 43, 2002, págs. 50-61.

BAGNOLI, M. / WATTS, S.G.: «Competitive intelligence and disclosure», *The RAND Journal of Economics*, Vol. 46, No. 4 (Winter 2015), págs. 709-729.

BAJO FERNÁNDEZ, M. / Bacigalupo Saggese, S.: Derecho penal económico, 2.ª ed., Editorial Universitaria Ramón Areces, Madrid, 2010.

BRADLEY, T.: «McAfee: Corporate Espionage is the Currency of Cybercrime», *PcWorld*, 28/3/2011.

CARBONELL MATEU, J.C. / GONZÁLEZ CUSSAC, J.L.: «Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabi-

lidad del domicilio», en Vives Antón, T.S.: *Comentarios al Código Penal de 1995*, Tirant lo Blanch, Valencia, 1996, págs. 990-1022.

Carrasco Andrino, M.ªM.: *La protección Penal del Secreto de Empresa*, Cedecs Editorial, Barcelona, 1998.

Castro Moreno, A.: «El derecho penal español ante el espionaje industrial y el secreto de empresa (artículos 278-280 CP)», en *RTDPE (Rivista Trimestrale di Diritto penale dell'Economia)*, I-2/2006, págs. 17-64.

Chan, M.: «Corporate Espionage and Wordplace Trust/Distrust», Journal of Business Ethics, Vol. 42, No. 1 (Jan., 2003).

Corcoy Bidasolo, M.: «Capítulo IX. De los daños», en Corcoy Bidasolo, M. / Mir Puig, S. (dirs.): *Comentarios al Código penal. Reforma LO 5/2010,* Tirant lo Blanch, Valencia, 2011.

Cowperthwait, T.S.: «Businesses Must Protect Against Cyber-Espionage», en *Connecticut Law Tribute*, vol. 37, n.º 11, 2011.

Dreyfuss, R.C. / Strandburg, K.J. (eds.): *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*, Edward Elgar, Cheltenham (UK)-Northampton (MA, USA), 2011.

Esteve Mora, F.: «La inteligencia económica», en *El País*, 25 de julio de 2013.

Estrada i Cuadras, A.: *Violaciones de secreto empresarial. Un estudio de los ilícitos mercantiles y penales*, Atelier, Barcelona, 2016.

Faraldo Cabana, P.: *Las Nuevas Tecnologías en los Delitos contra el Patrimonio y el Orden Socioeconómico*, Tirant Lo Blanch, Valencia, 2009.

Federal Bureau of Investigation (FBI) de los Estados Unidos: «Spear Phishers: Angling to Steal Your Financial Info», publicación del 4 de enero de 2009.

Fernández Díaz, C.R.: «La lista de clientes como objeto del secreto empresarial», *Revista Aranzadi Doctrinal*, núm. 7 (julio de 2016).

Fernández Díaz, C.R.: «La finalidad de descubrir un secreto de empresa en el delito de espionaje empresarial», *Revista General de Derecho Penal*, 26 (2016).

Giavazzi, S.: *La tutela penale del segreto industriale*, Giuffrè Editore, Milano, 2012.

González Cussac, J.L.: «Inteligencia jurídica: el valor estratégico del derecho en la seguridad económica», en *Cuadernos de Estrategia*

162-La inteligencia económica en un mundo globalizado, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2013, págs. 103-133.

GONZÁLEZ CUSSAC, J.L.: «Tecnocrimen», en GONZÁLEZ CUSSAC, J.L. / Cuerda Arnau, M.L. (dirs.): *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant lo Blanch, Valencia, 2013.

GUALDONI, F.: «La hora de la inteligencia económica», en *El País*, 26 de octubre de 2014.

GUTIÉRREZ FRANCÉS, M.L.: «Delincuencia económica e informática en el nuevo código penal», en GALLARDO ORTIZ, M.A.: *Ámbito jurídico de las tecnologías de la información*, Consejo General del Poder Judicial, Madrid, 1996.

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

HÖRNLE, T.: «Subsidiariedad como principio limitador. Autoprotección», en VON HIRSCH, A. / SEELMANN, K. / WOHLERS, W. (ed. Alemana) y ROBLES PLANAS, R. (ed. Española): *Límites al Derecho penal. Principios operatives en la fundamentación del castigo*, Atelier libros jurídicos, Barcelona, 2012.

HOROWITZ, R.: «Competitive Intelligence, Law, and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time)», en *Strategic and Competitive Intelligence Professionals (SCIP)*, volume 14-number 3, July-September, 2011.

INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA): «Descubre los diferentes tipos de malware que pueden afectar a tu pyme», publicado el 9 de mayo de 2016.

INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA): «Guía de almacenamiento seguro de la información», 2016.

INFOSEC INSTITUTE: «Duqu 2.0.: The Most Sofisticated Malware Ever Seen», June 17, 2015.

INSTITUTO GEOGRÁFICO NACIONAL DEL MINISTERIO DE FOMENTO: *Geoportal de metadatos de información geográfica*.

INSTITUTO NACIONAL DE ESTADÍSTICA (INE): *Empresas activas*, 2017.

JAVERS, E.: «Secrets and Lies: Rise of Corporate Espionage in a Global Economy», Georgetown Journal of International Affairs, Vol. 12, No. 1 (winter/spring 2011), págs. 53-60.

Lampe/Lenckner/Stree/Tiedemann/Weber: *Alternativ-Entwurf eines Strafgesetzbuches. Besonderer Teil. Straftaten gegen die Wirtschaft*, Tübingen 1977.

Larriba Hinojar, B.: «Ciberespionaje económico: Una amenaza real para la Seguridad Nacional en el siglo xxi», en González Cussac, J.L. / Cuerda Arnau, M.L. (dirs.): *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Tirant lo Blanch, Valencia, 2013.

Marrs, S.: «Inside Story on Trade Secrets: Protective measures are necessary to preserve a company's vital information», *ABA Journal*, Vol. 86, No. 10 (october 2000).

Martínez-Buján Pérez, C.: *Delitos relativos al secreto de empresa*, Tirant Lo Blanch, Valencia, 2010.

Ministerio de Economía y Competitividad: *Estrategia española de ciencia y tecnología y de innovación 2013-2020*.

Ministerio de Industria, Energía y Turismo: *Estadísticas PYME. Evolución e indicadores*, n.º 14, febrero 2016.

Mir Puir, S.: *Derecho penal. Parte general*, 10.ª edición, editorial Reppertor, Barcelona, 2016.

Morales Prats, F.: «Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Quintero Olivares, G. (dir.) / Morales Prats, F. (coord.): *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi-Thomson Reuters, Navarra, 2016.

Morón Lerma, E.: *El secreto de empresa. Protección penal y retos que plantea ante las nuevas tecnologías*, Aranzadi, Pamplona 2002.

Morón Lerma, E.: «Quiebras de la privacidad en escenarios digitales: Espionaje industrial», en *InDret*, núm. 21, 2007.

Olier Arenas, E.: «Inteligencia estratégica y seguridad económica», en *Cuadernos de Estrategia 162-La inteligencia económica en un mundo globalizado*, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2013.

Orts Berenguer, E. / Roig Torres, M.: *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch «colección de delitos», Valencia, 2001.

Palop Marro, F.: «La inteligencia para competir: nuevo paradigma en la dirección estratégica de las organizaciones en un mundo globa-

lizado», en *Cuadernos de Estrategia 162-La inteligencia económica en un mundo globalizado*, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2013.

PATTERSON, T.: «Chinese cyber spies may be watching you, experts warn», en *CNN*, de 28 de agosto de 2016.

PÉREZ DEL VALLE, C.: «La revelación de secretos de empresa por persona obligada a reserva (art. 279 CP)», *Cuadernos de Derecho* Judicial, n.º 14, 1997.

PICOTTI, L.: «Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale», en *Diritto dell'internet*, n.2/2005, págs. 189-204.

POOLEY, J.H.A.: *Trade Secrets. A guide to protecting Proprietary Business Information*, American Management Association, New York, 1987.

PRATS, J.M.: «Descubrimiento y revelación de secretos de empresa en el Código penal de 1995», en DEL ROSAL BLASCO, B.: *Delitos relativos a la Propiedad Industrial, al Mercado y a los Consumidores*, CGPJ, Madrid, 1997, págs. 169-207.

PRIETO DEL PINO, A.M.: *El Derecho Penal ante el uso de información privilegiada en el Mercado de Valores*, Thomson Aranzadi, Navarra, 2004.

RASCOFF, S.J.: «The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections», *The University of Chicago Law Review*, Vol. 83, No. 1 (Winter 2016), págs. 249-269.

RIBAGORDA GARNACHO, A.: «Seguridad de las tecnologías de la información», en *Ámbito jurídico de las tecnologías de la información,* CDJ, CGPJ, 1996.

SCHÜNEMANN, B.: «Cuestiones básicas de dogmática jurídico-penal y de política criminal acerca de la criminalidad de empresa», *Anuario de derecho penal y ciencias penales*, Tomo 41, Fasc/Mes 2, 1988.

SEGAL, A.: «Curbyng Chinese Cyber Espionage», en *Council on Foreign Relations (CFR)*, de 9 mayo de 2011.

SIMON, S.: «The Economic Espionage of 1996», *Berkeley Technology Law Journal*, Vol. 13, No. 1, Annual Review of Law and Technology (1998), págs. 305-317.

SUBRAMANIAN, R. / ISHAK, S.T.: «Competitor Analysis Practices of US Companies: An Empirical Investigation», *MIR: Management International Review*, Vol. 38, No. 1 (1st Quarter, 1998), págs. 7-23.

Suñol Lucea, A.: *El Secreto Empresarial. Un Estudio del Artículo 13 de la Ley de Competencia Desleal*, Thomson Reuters, Civitas, Pamplona, 2009.

Vilas Rodríguez, J.: «La contrainteligencia en el sector de la industria», *Economía Industrial*, n.º 405, 2017 (ejemplar dedicado a: Nuevas tecnologías digitales), págs. 133-141.

Walker, M.: «Should Intelligence Support to Private Industry Enhanced?», *Georgetown Journal of International Affairs*, Vol. 12, No. 1 (winter/spring 2011), págs. 8-15.

Warusfel, B. : « L'intelligence juridique, complément nécessaire de l'intelligence économique », en *Rue Saint Guillaume, n.º 162 (Dossier : À quoi sert l'intelligence économique ?*), mars-avril, 2011.

Young, C.: McAfee Raises the Stakes Against Cyberespionage», *McAfee*, 3/5/2017.

Zheng, Z. / Fader, P. / Padmanabhan, B.: «From Business Intelligence to Competitive Intelligence: Inferring Competitive Measures Using Augmented Site-Centric Data», *Information System Research,* Vol. 23, No. 3, Part 1 of 2 (september 2012), págs. 698-720.