LA CONTRAINTELIGENCIA EN EL SECTOR DE LA INDUSTRIA

JORGE VILAS RODRÍGUEZ

Instituto de Ciencias Forenses y de la Seguridad
Universidad Autónoma de Madrid

Debido a la globalización, la economía ejerce una importancia esencial en las relaciones internacionales y en la defensa de los intereses de Estados y empresas. El paso de la antigua economía de subsistencia, basada en el dominio de la tierra, a la actual economía meramente financiera, sitúa a la misma en el centro de innumerables conflictos regionales

y globales: la denominada guerra económica. Este término, puede no resultar del todo apropiado debido a su carácter netamente militar, pero, sin embargo, ejemplifica claramente la importancia de la economía en las disputas internacionales. Por tanto, la guerra económica, se concreta en acciones violentas realizadas por ciertos Estados o empresas con la finalidad de conquistar o proteger, bien un mercado, bien una posición de dominio económico. La economía se transforma, por tanto, en una especie de brazo armado para consolidar o aumentar posiciones de predominio en el mercado con instrumentos tales como: *benchmarking* ofensivo; acciones de influencia y *lobby*; políticas de precios, recortes o incrementos en el suministro de materias primas; control de normativas y regulaciones internacionales; manipulaciones de divisas, etc. (Olier Arenas, 2016).

Sin embargo, en un momento en el que las fronteras financieras han desaparecido y las económicas se encuentran en proceso de apertura, la geoeconomía se consolida como punto de encuentro de los intereses geopolíticos con la economía global, lo cual alcan-

za conflictos en relación con: las materias primas, el funcionamiento de los mercados, los intereses antagónicos en los organismos supranacionales, los desequilibrios de la globalización, las disputas monetarias, los intereses en los mercados de reciente aparición, los conflictos en aquellas regiones estratégicas de la economía global, las migraciones, el papel desempeñado por empresas transnacionales en la economía mundial, o los enfrentamientos por la supremacía en el ciberespacio (Olier Arenas, 2016).

En este escenario geoeconómico desarrolla sus mecanismos de acción la inteligencia económica, mecanismos que consisten en: analizar las previsiones económicas en entornos competitivos de gran complejidad, comprender el contexto político y geoestratégico en el que se desenvuelven; obtener un conocimiento exacto de las situaciones legales y regulatorias; valorar los intereses de la política exterior, así como de las relaciones internacionales que puedan condicionar su valoración; elaborar acciones estratégicas; establecer un seguimiento y controlar que se están cumpliendo los objetivos; evitar amenazas y riesgos; desarrollar criterios y sistemas de seguridad (ya sea física o virtual)

adecuados; e iniciar acciones económicas como elementos de ataque o defensa a favor de los intereses del Estado o de la empresa (Olier Arenas, 2016).

El objetivo de las políticas gubernamentales de inteligencia económica es fomentar entre las empresas la necesidad de implantación de planes y programas de inteligencia para conseguir una ampliación de la competitividad nacional. Del mismo modo, el uso de la inteligencia por parte de las empresas ayuda a mantener la seguridad económica nacional. Al igual que la inteligencia económica, la inteligencia competitiva consta de dos dimensiones complementarias: ofensiva y defensiva (Carvalho y Esteban, 2012).

La inteligencia competitiva ofensiva abarca la búsqueda y el análisis de información de interés. Además, incluye tanto la planificación como el desarrollo de acciones de influencia que puedan dirigir el comportamiento o la actuación de públicos y organizaciones, con la finalidad de conseguir los objetivos estratégicos y apoyar la estrategia organizacional. Países y organizaciones pueden, en cierto modo, influir en su entorno obteniendo pingües beneficios. Esta capacidad les permite construir su propia imagen, así como la de sus productos o marcas. Los programas de influencia, por tanto, van dirigidos a la formación del público, la divulgación de mensajes adecuados y la obtención de un reconocimiento por parte de personas o grupos de influencia en asuntos de interés para el Estado o la empresa en cuestión (Carvalho y Esteban, 2012).

La inteligencia competitiva defensiva se refiere a aquellas acciones relacionadas con la seguridad integral, la contrainteligencia y el apoyo legal en situaciones de conflicto. Además, un programa de inteligencia competitiva debe incluir también la implantación de medidas de protección de la información, lo que afecta a varios aspectos tales como el personal, las instalaciones, los equipos informáticos, las comunicaciones, la marca o la imagen. Las empresas, al igual que los Estados, deben salvaguardar su conocimiento sensible e implantar sistemas de defensa contra la intrusión de terceros (Carvalho y Esteban, 2012).

LA CONTRAİNTELIGENCIA: ¿QUÉ ES? ↓

La contrainteligencia, según palabras del profesor Esteban Navarro, se define como aquel conjunto de «actividades dirigidas a anular el conocimiento que los servicios de inteligencia extranjeros tratan de adquirir sobre aspectos esenciales del Estado en los ámbitos político, económico o de seguridad» (Esteban Navarro, 2007). Ésta se trataría de una definición clásica de la contrainteligencia, relacionada con las actividades militares y heredera del modelo norteamericano de la Guerra Fría (Andrade Quevedo, 2016).

En un mundo como en el que hoy vivimos, definido por el profesor Zygmunt Bauman como «líquido», en el cual la línea entre el poder y el Estado es cada vez más difusa, las empresas multinacionales ejercen muchas de las tareas que hasta ahora eran propiedad exclusiva del

Estado como, entre otras, tareas de inteligencia y contrainteligencia, dirigidas a defender sus propios intereses (Bauman, 2006; Bauman, 2013). De hecho, la privatización de la inteligencia es un hecho reciente que se ha visto potenciado por la aparición de nuevas amenazas y la ampliación del concepto de seguridad. Además, la privatización de la inteligencia se encuentra también relacionada con la creciente importancia de la seguridad económica, la cual sitúa a las empresas privadas como elementos claves para su mantenimiento (Carvalho y Esteban, 2012). Concretamente, en el ámbito empresarial, según se cita en el Diccionario de Inteligencia y Seguridad «la contrainteligencia se encamina a velar por la protección de la información y el conocimiento de la empresa de ataques y accesos no deseados, así como a blindar los secretos empresariales; puesto que todas las empresas cuentan con competidores interesados en conocer sus planes» (Díaz Fernández, 2013).

La contrainteligencia no se debe entender como algo separado del proceso de elaboración de inteligencia, sino como un elemento más del proceso que está presente en todo momento (Lowenthal, 2006). Entre sus distintas tareas, el *Glosario de Inteligencia* enumera las siguientes: el control del personal que se incorpora a una organización y de aquel que disponga de acceso a la información sensible; la creación de una cultura de seguridad entre las personas encargadas del manejo de información; la vigilancia de conductas inapropiadas en el personal de la organización; la identificación y vigilancia de los miembros de otras organizaciones; el conocimiento del modo de operar de dichas organizaciones; la realización de actividades de contrainformación; etc. (Esteban Navarro, 2007). Como se puede observar, son tareas que no nos sorprenden, o no debería, fuera del ámbito de los servicios de inteligencia; se trata de tareas que, hoy en día, son asimiladas por las grandes empresas multinacionales. Cabe resaltar, además, el aspecto de que las acciones hostiles pueden provenir de organizaciones «amigas» e, incluso, desde el interior de la propia organización (Esteban Navarro, 2012).

En definitiva, el rol de la contrainteligencia es muy completo y activo en el proceso de inteligencia, ya que está directamente relacionada con las tareas de seguridad (entre las que se incluyen investigaciones sobre áreas vulnerables de la propia organización) y, además, también debe estar en contacto con la parte productora de inteligencia para detectar los actores que podrían estar interesados en la inteligencia propia (Andrade Quevedo, 2016).

LA SEGURIDAD DEFENSIVA Y EL CONTRAESPIONAJE ↓

La contrainteligencia presenta, básicamente, dos ámbitos de actuación: la seguridad defensiva y el contraespionaje.

Seguridad defensiva ↓

La seguridad defensiva consiste en proteger las instalaciones con la finalidad de impedir la intrusión, prote-

ger al personal frente a posibles amenazas, velar por el correcto desenvolvimiento de aquellas operaciones en desarrollo y preservar el conocimiento sensible. Para llevar a cabo estas tareas se utilizan tres grandes métodos; la seguridad física, la seguridad técnica y la seguridad del personal, cada una de las cuales cuenta con sus técnicas específicas (Wettering, 2000). En términos de seguridad, el éxito se establece en función de si se ha producido o no una infiltración. Si ésta se produce, no solo provoca una pérdida de información comprometiendo las operaciones, sino que ocasiona daños en la moral y en el prestigio de la organización (Esteban Navarro, 2012).

Para preservar la seguridad física de las instalaciones y sus documentos, con la finalidad de evitar el acceso de aquellas personas sin autorización, se establecen medidas tales como defensas estáticas, vallas, alarmas, sistemas de videovigilancia, guardias de seguridad, camuflaje de instalaciones y vehículos, identificación y control de visitantes, restricciones de acceso, uso de contraseñas, inspecciones oculares, identificación de personas, escaneo y apertura de equipajes, controles de seguridad periódicos, etc. (Esteban Navarro, 2012).

En cuanto a las contramedidas de seguridad técnica, éstas se refieren al conjunto de técnicas empleadas para la detección de infiltraciones, ya sean escuchas, seguimiento de movimientos, interceptación de comunicaciones, etc. Algunas de las técnicas más utilizadas son el escaneo del espectro radioeléctrico y las medidas de seguridad informática (infosec) y de comunicaciones (comsec), siendo estas dos últimas las más importantes. En cuanto a las medidas de seguridad informática éstas pretenden impedir intrusiones en redes o sistemas, así como el acceso de personal no autorizado a almacenes digitales. En lo que respecta a las comunicaciones, se emplean teléfonos y otros sistemas de transmisión de información que no pueden ser interceptados con facilidad y, principalmente, se lleva a cabo el cifrado de los mensajes (Esteban Navarro, 2012).

Por último, con respecto a la seguridad del personal, que persigue un uso responsable de los secretos por parte de los individuos que tienen acceso a los mismos, existen dos principios que establecen la relación del personal con la información: la compartimentación y «la necesidad de saber». La compartimentación se refiere a la restricción del acceso a un secreto a aquellas personas autorizadas mediante acreditaciones de seguridad que determinan la información a la que pueden acceder, para tratar de evitar una posible fuga de información. En cambio, «la necesidad de saber» determina que un empleado sólo puede tener acceso a aquella información imprescindible para realizar su trabajo, aunque esto último podría resultar contraproducente si se priva a un empleado del conocimiento de una información relevante para su trabajo (Lowenthal, 2006). Además de una educación continua del personal en materia de seguridad, una medida complementaria para evitar filtraciones, pérdidas

o robos, suele ser la prohibición de sacar documentos de las instalaciones destinadas a su uso (Esteban Navarro, 2012).

En cuanto al personal, pueden emplearse, además, determinadas medidas de seguridad orientadas a detectar vulnerabilidades o conductas inadecuadas en los empleados que puedan ser aprovechadas por el adversario. Estas medidas incluyen la investigación del perfil de los candidatos y el seguimiento de su estilo de vida, así como la monitorización de su teléfono móvil o su correo electrónico (Esteban Navarro, 2012). Estas últimas medidas, intrusivas de la intimidad, están pensadas para los servicios de inteligencia, si bien la monitorización del correo corporativo de los empleados sí que debería ser una acción generalizada para evitar su mal uso y posibles filtraciones en el ámbito de la empresa privada.

Contraespionaje

El contraespionaje consiste en identificar adversarios y obtener un conocimiento exhaustivo sobre las operaciones que se están planificando o desarrollando con el fin de evitar su ejecución. Se pretende conocer la estructura organizativa del adversario, su personal clave, sus formas de reclutamiento y formación, sus instalaciones, sus medios, etc. Idealmente se busca que el personal de contrainteligencia consiga el bloqueo de las actividades de su adversario mediante la infiltración o penetración en el mismo. El espía infiltrado debe tratar de situarse en lo alto de los órganos de responsabilidad de las organizaciones enemigas, puesto que es en estos ámbitos donde se maneja el grueso de la información más relevante y confidencial. El proceso de infiltración es lento y conlleva un alto riesgo. El infiltrado debe ganarse la confianza del personal de la organización enemiga y abrirse paso sin levantar sospechas hasta conseguir la información que desea (Esteban Navarro, 2012). La infiltración es una actividad habitual y con apoyo legal en los servicios de inteligencia, sin embargo, en el ámbito privado, se trata de una actividad ilegal además de poco ética.

Las técnicas empleadas para llevar a cabo la infiltración en el adversario son de distintos tipos. Lo más deseable es el reclutamiento de un agente que forme parte de la organización en la que nos queremos infiltrar, es decir, un «agente en plaza». Es también de gran utilidad disponer de «agentes durmientes», que permanecen inactivos durante largo tiempo hasta que se recurre a ellos. En cuanto a los motivos más habituales que inducen al personal adversario a colaborar con nuestra organización se encuentran los económicos, aunque, en general, el motivo de la traición suele ser una conjunción de diversos factores. Cuando esta traición se produce en nuestra propia organización, urge llevar a cabo una evaluación de los daños determinando la información que ha sido comprometida (Esteban Navarro, 2012).

Otro método del contraespionaje es la decepción o contrainformación, consistente en dar al adversario una falsa impresión sobre algo, de manera que éste

actúe en contra de sus intereses. Sus rasgos definitorios son el disimulo, la manipulación, la distorsión, la intoxicación y la falsificación. Ésta no se debe confundir, sin embargo, con la desinformación, que pretende engañar a la opinión pública. La contrainformación es una operación complicada que requiere conocer detalladamente los medios a través de los cuales el enemigo obtiene y analiza la información (Esteban Navarro, 2007; Esteban Navarro, 2012).

El interrogatorio es otro importante método del contraespionaje (Esteban Navarro, 2012), pero el más habitual es la vigilancia, llevada a cabo de forma continua y subrepticia tanto sobre organizaciones «amigas» como enemigas. En palabras atribuidas a Henry Kissinger, «no existen servicios de inteligencia amigos, sino servicios de inteligencia de países por el momento amigos» (Lowenthal, 2006).

El contraespionaje, a pesar de plantear cuestiones legales y éticas, podría conceptualizarse como la función más precisa y sofisticada de todas las funciones de inteligencia (Esteban Navarro, 2012; Prunckun, 2012).

Debido al surgimiento de las amenazas asimétricas, la ampliación del concepto de seguridad y el auge de la inteligencia económica, gran parte del conocimiento obtenido por empresas y organizaciones alcanza la categoría de secreto; y, a pesar de que su protección es responsabilidad del organismo en cuestión, los servicios de inteligencia también se implican activamente en su protección (Esteban Navarro, 2012).

EL ESPIONAJE: LA GRAN AMENAZA DEL SECTOR

El espía es aquella persona que, al servicio de una organización, obtiene, de forma encubierta, información secreta, reservada, de carácter político, económico, industrial, tecnológico, militar, etc., relativa a otra organización (Prieto del Val, 2016). La primera referencia histórica sobre el empleo de espías se encuentra en una tablilla del año 2210 a.C., en la que se pone de manifiesto que ya el rey Sargón I utilizaba mercaderes como espías durmientes. También, durante el Imperio Azteca (s. XIV) se tiene constancia de la existencia de este tipo de espías, unos comerciantes que constituían la avanzada en las operaciones de conquista (Herrera Hermosilla, 2012). Se puede mencionar, también, el caso del espía Jorge Juan, a quien el marqués de la Ensenada encargó una misión en Londres en la cual debía obtener toda la información posible sobre construcción y armamento naval; organizar una fuga de material humano contratando secretamente a constructores, especialistas, técnicos y obreros cualificados en dichas materias; adquirir instrumentos y documentación; hacerse con planos sobre todo tipo de barcos, arsenales, puertos, fortificaciones, etc. (Prieto del Val, 2016).

El vocablo «espíar» quiere decir observar, vigilar cuidadosamente con algún propósito, haciendo uso del disimulo y el engaño. Es fácil darse cuenta de la gran

ventaja que supone saber, como decía Clausewitz, «lo que hay detrás de la colina», es decir, conocer todo lo posible en relación con el enemigo. El conocimiento de esta información constituye, ya desde tiempos remotos, un elemento clave para la toma de decisiones en el ejercicio del poder, pero en la actualidad, el espionaje se ha convertido en una actividad imprescindible en los ámbitos político, militar y económico (Martínez Laínez, 2016).

El espionaje es una de las amenazas a las que tiene que hacer frente la contrainteligencia y, de manera especial, en el sector de la Industria, ya que la capacidad de innovación frente a los competidores constituye el bien más preciado en el ámbito de la competencia económica (Cozzi y Spinesi, 2006). Dicha capacidad de innovación se ha convertido en un objeto especialmente codiciado por los competidores, de manera que ha tenido que ser puesta bajo una intensa protección legal. Para ello, la innovación realizada puede caer dentro de la categoría de secreto, si la empresa considera que su valor radica en su desconocimiento por parte de los competidores; o bien registrarse públicamente en forma de patente, marca, nombre comercial, etc. (Ruiz Rodríguez, 2016).

Para reducir la ventaja competitiva que supone dicha capacidad de innovación, el competidor puede echar mano de dos tipos de recursos: legales o ilegales. Entre los recursos legales se encuentra la inversión en I+D+i, los acuerdos económicos con el competidor para compartir conocimiento, la expulsión del innovador del mercado mediante, por ejemplo, el lanzamiento de una OPA (Oferta Pública de Adquisición) que fusione a los competidores, etc. En cuanto a los recursos ilegales, el más frecuente es el espionaje industrial (Ruiz Rodríguez, 2016).

El espionaje industrial es una conducta ilegal que se desarrolla en un contexto de relaciones económicas en las que cualquiera se puede convertir en autor o víctima del mismo. Su objetivo es desvelar el secreto de empresa de una organización competidora mediante conductas ilegales. El secreto de empresa se trata de una información secreta, que lo es porque el dueño manifiesta una voluntad de que así lo sea y porque tiene un valor económico para la empresa y lo puede tener para los competidores. La ilegalidad de estas conductas no depende del valor económico del secreto desvelado, por lo que el espionaje industrial hace referencia a la revelación de cualquier tipo de información referente a la empresa competidora que ésta guarde para sí, como una simple lista de proveedores, un diseño de última generación, innovaciones tecnológicas no registradas, los precios de adquisición de productos, los márgenes de ganancias, etc. (Martínez-Buján Pérez, 2010; Ruiz Rodríguez, 2016).

El espionaje industrial, como actividad ilícita, debe ser, claramente, diferenciado de las acciones de inteligencia competitiva. El «Diccionario LID de Inteligencia y Seguridad» delimita claramente los conceptos, al definir el espionaje industrial como la «acción delicti-

va encaminada a obtener información confidencial y valiosa de una empresa competidora» que «engloba acciones tales como el chantaje, el robo de secretos comerciales, la intromisión en las comunicaciones o la corrupción» (Díaz Fernández, 2013).

EL CIBERESPIONAJE: ESPIONAJE 2.0 ↓

En la actual «sociedad de la información» sería un grave error no tratar el asunto del ciberespionaje. Hasta ahora, se ha tratado el lado humano de la contrainteligencia, la cual no hay que desdeñar. Sin embargo, las Tecnologías de la Información y la Comunicación (TIC) han revolucionado todos los ámbitos de la sociedad y la inteligencia no ha sido inmune a estos cambios. Este gran desarrollo tecnológico contribuye al crecimiento económico de las naciones y ofrece una gran oportunidad de evolucionar y progresar a los países menos desarrollados. Al mismo tiempo, la idea de un ciberespacio abierto favorece la integración social, así como las libertades y los derechos fundamentales de los individuos. No obstante, a pesar de las ventajas que ofrece la progresiva evolución de las tecnologías, ésta genera, a su vez, nuevos retos para la seguridad de los individuos, las empresas y los Estados (Tejada y Martín, 2016).

En este contexto, surge el concepto de ciberdelincuencia, que hace referencia a una manera de perpetrar acciones ilegales cuyo denominador común es su estrecha relación con las TIC, ya sea porque éstas constituyan el objeto del delito o porque sean el medio a través del cual éste se perpetra (Tejada y Martín, 2016). Los ciberdelitos más comunes son: el acceso ilegal a sistemas ajenos, la interceptación ilegal, la interferencia de datos y sistemas, la pornografía infantil, los delitos contra la propiedad intelectual y el fraude económico (González y Larriba, 2011). Una modalidad de ciberdelincuencia es el ciberespionaje, que busca acceder de forma no autorizada a redes, sistemas o repositorios de información estratégica (Navarro Bonilla, 2014).

A nivel empresarial, hace unos años que el ciberespionaje está en auge y se ha consolidado como una práctica común (Morant y López, 2013). Es innegable que la información ha adquirido recientemente un gran valor y su seguridad es cada vez más importante (Rego Fernández, 2016). Por todo ello, la seguridad de la información, «el área relativa al desarrollo e implementación de contramedidas de seguridad de todo tipo [...] para mantener la información [...] libre de amenazas» (Cherdansteva y Hilton, 2013), se presenta como un factor clave. Entre las técnicas empleadas para proteger esta información se encuentran los algoritmos matemáticos y criptográficos, los sistemas informáticos y de telecomunicaciones o los procedimientos legales y normativos (Rego Fernández, 2016).

El espionaje, hoy en día, se define por la gran accesibilidad que ofrece la informática (Olier Arenas, 2013), y, es posible que, en un futuro, se produzca un cambio del espionaje masivo estatal al microespionaje (Navarro Bonilla, 2014). Internet se ha convertido en una

herramienta clave para los espías económicos, que la emplean, principalmente, para la obtención de información reservada (González y Larriba, 2011).

Como consecuencia del uso generalizado de las TIC, los diversos ataques, así como su intensidad, son muy dispares. Algunos de estos consisten en accesos no autorizados, *bots*, infección de equipos de forma remota, captura de contraseñas, extorsiones, desfiguración de páginas web, *phishing*, ataque de denegación de servicios, uso de *malwares*, explotación de servidores, robos de dispositivos, etc. (González y Larriba, 2011).

Para minimizar estos riesgos, es necesario implantar medidas que protejan la información sensible, ya sea mientras ésta se encuentra almacenada o en tránsito. Para proteger la información almacenada es de gran utilidad el empleo de sistemas criptográficos. Estos sistemas garantizan tanto la confidencialidad (mediante su cifrado) como la integridad de la información (protección con firmas digitales) y, dichas técnicas, también son útiles para la protección de la información en tránsito. La incorporación de listas de acceso, la realización de copias de seguridad o la inclusión de mecanismos de autenticación también son de gran ayuda para proteger la información almacenada (Rego Fernández, 2016).

Por último, también es posible proteger la información sin actuar directamente sobre ella, mediante sistemas e infraestructuras tecnológicas robustas. Gracias a todas estas técnicas, es posible minimizar el riesgo de sufrir incidentes, pero es prácticamente imposible prevenir todas las amenazas (Morant y López, 2013).

Sin embargo, pese a que los recientes avances tecnológicos permiten acceder con escaso riesgo a cantidades ingentes de información, el factor humano es todavía imprescindible para tomar las decisiones correctas, ya que éstas requieren valoración y conocimiento humano en base a la información encontrada, más allá de lo que pueda captar una máquina (Navarro Bonilla, 2014; Martínez Lainez, 2016).

LA INTELIGENCIA COMPETITIVA Y ECONÓMICA: ¿PARA QUÉ? ↓

En el contexto de la globalización han surgido nuevas formas de ataque a los intereses económicos de empresas y Estados. Dichos ataques pueden proceder tanto del interior como del exterior de la organización y se inscriben en un contexto en el que intervienen múltiples agentes. En este sentido, el *Federal Bureau of Investigation* (FBI) considera que las actividades de espionaje económico perpetradas por compañías extranjeras, para tratar de buscar una buena posición en las negociaciones con multinacionales occidentales, pueden constituir un riesgo o amenaza para la seguridad nacional, de ahí que estas actividades se incluyan como una de las siete materias de la *National Security Issues Threat List* en las que se requiere acometer acciones de inteligencia (González y Larriba, 2011).

La necesidad de obtener información sobre la competencia y sobre el entorno en el que ésta se mueve se ha convertido, con el fenómeno de la globalización, en uno de los objetivos prioritarios en relación a la supervivencia de una empresa, teniendo en cuenta que alrededor de un 75% del valor de una empresa reside en la información que ésta posee (González y Larriba, 2011).

La Inteligencia Económica, empleada por el Estado, se encarga de obtener y controlar la información para su posterior explotación por parte de los actores económicos, con la finalidad de alcanzar una mejor planificación estratégica que disminuya la incertidumbre (González y Larriba, 2011). Este tipo de inteligencia se apoya en actividades de vigilancia y contravigilancia; influencia y desestabilización; y protección del patrimonio informativo de las empresas (Bégin, Deschamps *et al.*, 2007). Además, la inteligencia económica también tiene como cometido sensibilizar a las empresas nacionales para que apliquen medidas de prevención contra el espionaje (Díaz Fernández, 2013). Para Alain Juillet, la inteligencia económica cumple tres funciones: promover la competitividad en el sector de la industria; reforzar la seguridad de la economía y de las empresas; y acrecentar la influencia de un país; y afirma, además, que la gestión de la información obtenida mediante la inteligencia económica es clave para la supervivencia y el desarrollo de las empresas (Juillet, 2006).

El conocimiento sobre los competidores y el entorno, de forma sistemática, se convierte en una herramienta de gran valor en el contexto de la economía global, ya que permite a las organizaciones adelantarse a los cambios y conseguir, así, una ventaja competitiva. Esto es lo que se denomina inteligencia competitiva, la cual debe proceder de fuentes abiertas (OSINT) y es necesaria para que las empresas lleguen a alcanzar un alto nivel de competitividad sin incurrir en acciones ilegales (Esteban Navarro, 2007; Díaz Fernández, 2013). En la Venecia del siglo XIII, sin haberse acuñado aún el término, ya se usaban métodos similares para proteger la industria gremial del vidrio, manteniendo en la confidencialidad sus fórmulas secretas (Izquierdo Triana, 2016).

La inteligencia económica y la inteligencia competitiva se deben compaginar con la conrainteligencia en los procesos de toma de decisiones, la defensa del capital intelectual, la gestión del riesgo de la empresa o la realización de actividades de presión o *lobby* (González y Larriba, 2011). Dichos procesos tienen como objetivo abordar dos ámbitos: el ofensivo, que pretende acrecentar la influencia y la competitividad de la empresa; y el defensivo, que procura evitar que crezca para proteger sus activos tanto tangibles como intangibles (la marca, el I+D+i, el *know-how*). Ejemplos del primero son las evaluaciones de competidores, los análisis de cambios regulatorios, las acciones de desinformación, las labores de *lobby* o reconocimiento de patrones y relaciones. Ejemplos del ámbito defensivo son las labores de conrainteligencia, las investigaciones de competencia desleal, la contratación de di-

rectivos clave, la reducción de riesgos en una fusión o adquisición, la protección de sistemas de información y la prevención de riesgos (Izquierdo Triana, 2016).

Cabe mencionar que, en cierto modo, el espionaje económico e industrial se considera el lado oscuro de la inteligencia económica y competitiva, ya que en el ejercicio de estas acciones es relativamente fácil traspasar la frontera entre lo legal y lo ilegal. Es indicativo de esto último que, algunas empresas, agotados los medios legales de obtención de información, contraten a agencias privadas para la obtención ilegal de información reservada (González y Larriba, 2011).

En definitiva, las principales diferencias existentes entre la inteligencia económica y competitiva y el espionaje económico e industrial radican en que las primeras utilizan procedimientos legales para la obtención de información y su objetivo es transformar dicha información en conocimiento útil que otorga beneficios a largo plazo, mientras que el segundo hace uso de métodos ilícitos para adquirir dicha información, su empleo no aporta ningún tipo de conocimiento y los beneficios se obtienen en un plazo inmediato. Además, el espionaje económico e industrial constituye un método de obtención de información, mientras que la inteligencia económica y competitiva se refiere a todo un proceso (González y Larriba, 2011).

La presencia de un entorno económico cada vez más competitivo, globalizado y deslocalizado, dificulta a la empresa la protección de sus activos tanto tangibles como intangibles. Sin embargo, el conocimiento obtenido en el proceso de Inteligencia Competitiva permite, si es adecuado, facilitar la toma de decisiones otorgando a la empresa una ventaja competitiva frente a sus competidores, además de ayudar, también, a la protección de dicha ventaja (Díaz Fernández; Izquierdo Triana, 2016).

LA VIGILANCIA: UNA PRÁCTICA ESENCIAL ¶

Es deber de una empresa estar siempre al tanto de lo que ocurre en el mercado e intentar prever los cambios que puedan surgir. Además, las leyes de libre competencia dificultan esta tarea obligando a las organizaciones a atender, no solamente a la economía o el comportamiento de los clientes, sino también a la normativa legal y la información sobre la competencia. La posesión de esta información, con frecuencia, otorga a la empresa una ventaja competitiva, pero para que ésta información sea de utilidad, es necesario transformarla en conocimiento útil para la toma de decisiones, lo que se consigue mediante un correcto análisis. Como consecuencia, la supervivencia de una empresa en el mercado se convierte en tarea complicada debido a dos problemas fundamentales: la ingente cantidad de información disponible y la dificultad de interpretarla correctamente. Debido al desarrollo de la tecnología digital y a la globalización de mercados y empresas, hoy en día, es posible acceder a cualquier clase de información en tiempo real (Larreira García, 2016).

Para evitar el exceso de información se debe recoger, filtrar, analizar y poner a disposición de las personas la información exacta, concreta y completa para la toma de decisiones. Este proceso de vigilancia tecnológica tiene cada vez más calado en las organizaciones y se entiende como un apoyo a la toma de decisiones estratégicas a todos los niveles de la empresa. La vigilancia tecnológica no es un proceso nuevo: el seguimiento de la competencia, el análisis de señales y la creación de una estrategia empresarial son inherentes a cualquier actividad económica en cualquier época, no obstante, faltaba una sistematización, un procedimiento y un orden: eso es la vigilancia tecnológica «moderna» (Larreina García, 2016).

La tarea, hoy en día, se presenta más fácil por el apoyo de consultores, herramientas de procesamiento digital o el acceso a las fuentes. Sin embargo, la falta de tiempo para encontrar y analizar la información y la dificultad para saber dónde encontrar aquella que se necesita, hacen que la ventaja sea mucho más pequeña. Para la implantación de un sistema de vigilancia tecnológica no es preciso contar con grandes *softwares* capaces de analizar información, ni destinar una serie de recursos económicos grandes. El primer paso de la vigilancia es saber cuáles son los factores críticos que hay que vigilar, es decir, aquellos factores que definen un negocio. El pilar de todo sistema de vigilancia tecnológica es el especialista humano, capaz de recoger la información según los factores críticos detectados y en el momento oportuno, y capaz de hacer un primer filtrado, separando la información relevante del «ruido», de clasificar los factores críticos, de la primera búsqueda, de la identificación de fuentes y repositorios, y por último, de la categorización y ordenación de resultados para su entrega a un analista o conjunto de analistas que conviertan esa información en conocimiento (Larreina García, 2016).

Entre las dificultades que se pueden encontrar está que las fuentes de información pueden ser de diferente naturaleza. La información que está en soporte digital puede ser de dominio público o de ámbito privado. Si es de dominio público, se puede acceder a esta información mediante herramientas que ya existen y que en la mayor parte de los casos son gratuitas. El problema sobreviene cuando la información se encuentra en el ámbito de lo privado. Ésta puede ser accesible sólo con una contraseña o presentar además un precio, que dependiendo de la información puede ser muy alto. Es en estos casos cuando se requiere verdaderamente la inversión de recursos; la información cuesta, y un trabajo de vigilancia no puede ser bueno si el sustrato no es bueno o es incompleto. Finalmente, y no es la menor de las dificultades, la información se encuentra disponible, pero dispersa. Un enjambre de portales temáticos, bases de datos de todo tipo de contenido, publicaciones y artículos digitales, *blogs* y foros de opinión, noticias a tiempo real, hemerotecas, páginas de la Administración, bases de patente, de proyectos de investigación, etc., hacen que el proceso de recogida y selección de la información sea lento, y de que no se tenga la certeza de ser, además,

exhaustivo. Se le suma que muchas de las fuentes son multi-formato o están en varios idiomas, o que la información puede ser heterogénea, estar desactualizada, no estar contrastada, o estar incompleta (Larreina García, 2016).

La vigilancia tecnológica nos aporta un doble beneficio; la anticipación a diferentes escenarios y la adecuación de las estrategias de la empresa a un entorno continuamente cambiante. Además, la vigilancia tecnológica es especialmente útil para llevar a cabo la monitorización de la competencia empleando exclusivamente medios lícitos de obtención de información, evitando toda forma de espionaje. Se puede hacer un seguimiento de la competencia en cuanto a sus desarrollos tecnológicos, los mercados en los que se mueve, quienes trabajan en ellos y dónde lo hacen; podemos determinar la evolución del interés en una tecnología, detectar tecnologías emergentes, aquellas que están quedando obsoletas o aquellas que provocan la aparición de otras o que son aplicables a otras áreas. Saliendo del campo puramente tecnológico, se puede conocer también qué tipo de perfiles está buscando una empresa (monitorizando portales de empleo), qué tipo de investigación quiere llevar al mercado (haciendo un seguimiento de ferias y congresos) o cuáles son sus últimos movimientos. No siempre es posible encontrar trazas de los movimientos de una empresa, pero lo importante está en dilucidar la estrategia de la empresa a través de esos retazos de información encontrados. La detección y análisis de las señales es una de las ventajas de la inteligencia competitiva (Larreina García, 2016).

LA PROPIEDAD INTELECTUAL E INDUSTRIAL ↓

Por secreto de empresa se entiende el conocimiento exclusivo de cualquier materia o información relativa a aspectos organizativos, contables, tecnológicos, etc., que una empresa guarda celosamente para sí. Se trata de materias, por tanto, que no han de ser de conocimiento general, y cuyo descubrimiento puede acarrear consecuencias perjudiciales para la empresa (Orts y González, 2004). El artículo 13.2 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, es la única norma jurídica española que utiliza el término «espionaje». Por su parte, el Código Penal español (texto de 1995) afronta las conductas propias del espionaje industrial en sus artículos 278 a 280. El artículo 278 tipificó por primera vez como delito los actos propios de espionaje industrial o empresarial. En concreto, establece que «el que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos, o electrónicos, soportes informáticos y otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses». Es decir, el secreto de empresa puede materializarse en todo género de soporte, tanto en papel como electrónico, tanto en original como en copia, comunicaciones verbales, las cifras, listados, partidas

contables, organigramas, planos, memorandos, etc. (González y Larriba, 2011; Ruiz Rodríguez, 2016).

El origen de la regulación moderna de las conductas que violan los secretos industriales se sitúa en la Inglaterra de los primeros momentos de la Revolución Industrial, que, frente a la fuga de especialistas, herramientas y maquinaria, que ofrecían una clara ventaja competitiva frente a Francia, se vio obligada a desarrollar una extensa legislación anti espionaje industrial cuyo primer exponente es la ley de 1718 contra la emigración de trabajadores cualificados al extranjero. El Convenio de París para la protección de la propiedad intelectual de 1883 se puede considerar, a su vez, el primer hito legal internacional para afrontar estas conductas (Ruiz Rodríguez, 2016).

Los instrumentos jurídicos orientados a legislar los derechos relativos a la propiedad intelectual e industrial se centran en proteger a una singular categoría de bienes jurídicos, la designada con la terminología «bienes inmateriales», manifestaciones de la invención, la capacidad creativa, el saber, el talento y, en general, el ingenio humano. De este modo se pretende asegurar que la inversión que en su día se dedicó a la innovación regrese a la empresa (Gómez Rivero, 2012).

Entre los sujetos activos del espionaje, estos pueden agruparse en dos clases: los que acceden al mismo, desde fuera o desde dentro de la empresa, sin obligaciones de reserva; y aquellos que por su situación tienen acceso a los secretos y se encuentran vinculados por un deber de confidencialidad. Estos sujetos, por su peculiar posición respecto al titular del secreto, son objeto de una regulación intensa (art. 279 del Código Penal) y su infracción conlleva sanciones más graves para los mismos (Ruiz Rodríguez, 2016). Entre los sujetos especialmente obligados a guardar sigilo se incluyen directivos, encargados, empleados, obreros, socios y administradores (González y Larriba, 2011).

Con todo, quizás convenga recordar que las iniciativas más recientes en materia de espionaje económico e industrial se inscriben en el marco de la necesidad surgida por plantear nuevos planes estratégicos para proteger a los países de las amenazas de la red, considerando la ciberseguridad como un elemento fundamental de la seguridad y considerando los asuntos económicos y los secretos de empresa como parte esencial del concepto de seguridad (González y Larriba, 2011).

Es destacable que, recientemente, la Unión Europea tramitó la «Propuesta de Directiva (COM 2013) relativa a la protección del saber hacer y la información empresarial no divulgada contra su obtención, utilización y divulgación ilícitas» (Ruiz Rodríguez, 2016). Dicha propuesta se ha aprobado con el siguiente nombre: «Protección de los secretos comerciales contra su obtención, utilización y divulgación ilícitas» el día 14 de abril de 2016 (1).

CONCLUSIONES ↓

Algunos Estados han adoptado abiertamente el espionaje industrial situando la competitividad económica en el núcleo de la «Razón de Estado» y no dudan en llevar a cabo conductas como el cibertaque para mantener la primacía económica mundial. A pesar de que se ha difundido la idea del libre mercado, ningún Estado confía en los actores económicos, por lo que, en la realidad dicha liberalización económica es parcial y el objeto real de la política económica es, en muchos casos, la protección de los intereses económicos nacionales. Algunos conceptos teóricos fundamentales de la economía de mercado, como el de la libre competencia, parecen quedar como simples enunciados abstractos, cuya traducción a la práctica es más que discutible (Ruiz Rodríguez, 2016).

Según palabras de Eduardo Trigo y Sierra, la falta de conciencia social industrial, existente en España, provoca un aumento de los casos de competencia desleal. Afirma que es de gran importancia contar con un sistema educativo que induzca a los jóvenes a apreciar el valor de los logros tecnológicos de su país y a aprender a respetarlos y protegerlos. El déficit cultural, unido a la ignorancia legal, incentiva la perpetración de numerosos actos ilegales y provoca una cierta sensación de permisividad. Dichos actos son impensables en países de nuestro entorno, donde la mayoría de la población asume que el aprovechamiento indebido de un secreto industrial, un listado de clientes o un acto de imitación son comportamientos muy graves (2).

La falta de peso de la industria española impide que la economía crezca de una forma sostenible, al depender excesivamente del sector terciario que, a su vez, es muy vulnerable ante, por ejemplo, oleadas de ataques terroristas, situaciones generalizadas de inseguridad, epidemias, y cualquier otra situación que genere miedo o pánico entre la población. Además, quede como muestra de la importancia de este sector que la suma de la construcción y servicios no emplean, en conjunto, ni la décima parte de inversión en I+D+i que la Industria. Por lo tanto, mientras no se incremente la actividad industrial, será imposible crear empleo estable y bien remunerado (3). Por todo ello, se debería proteger la industria española implantando medidas defensivas y ofensivas como las que nos aportaría un buen sistema de contrainteligencia especializado en la defensa de la industria nacional.

NOTAS ↓

- [1] <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0131&language=ES&ring=A8-2015-0199>
- [2] <http://www.farodevigo.es/economia/2016/08/13/eduardo-trigo-sierra-casos-competencia/1514800.html>
- [3] Véase nota 2.

BIBLIOGRAFÍA ▼

ANDRADE QUEVEDO, C. (2016) «*Contrainteligencia*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 65-72. Ed. Tirant lo Blanch. Valencia.

BAUMAN, Z. (2006) «*Vida líquida*». Ed. Paidós Ibérica. Barcelona.

BAUMAN, Z. (2013) «*Vigilancia líquida*». Ed. Paidós Ibérica. Barcelona.

BÉGIN, L., DESCHAMPS, J. Y MADINIER, H. (2007) «*Une approche interdisciplinaire de l'intelligence économique*». Cahier de l'Haute école de gestion de Genève. Ginebra.

CARVALHO, A. Y ESTEBAN NAVARRO, M.A. (2012) «*La privatización de la Inteligencia*». En, González Cussac, J.L. (dir.) «*Inteligencia*», pp. 198-214. Ed. Tirant lo Blanch. Valencia.

COZZI, G. Y SPINESI, L. (2006) «*Intellectual appropriability, product differentiation, and growth*». Macroeconomic Dynamics, Vol. 10, pp. 39-55. Cambridge University Press. Cambridge.

CHERDANTSEVA Y. Y HILTON J. (2013) «The 2011 survey of Information Security and information assurance professionals: findings». En Almeida, F. y Portela I., «Organizational, legal, and technological dimensions of IS administrator». IGI Global Publishing. Pennsylvania.

DÍAZ FERNÁNDEZ, A.M. (coord.) (2013) «*Diccionario LID Inteligencia y Seguridad*». LID Editorial. Ministerio de la Presidencia. Gobierno de España. Madrid.

ESTEBAN NAVARRO, M.A. (coord.) (2007) «*Glosario de Inteligencia*». Secretaría General Técnica. Ministerio de Defensa. Madrid.

ESTEBAN NAVARRO, M.A. (2012) «*Contrainteligencia y operaciones encubiertas*». En, González Cussac, J.L. (dir.) «*Inteligencia*», pp. 171-197. Ed. Tirant lo Blanch. Valencia.

GÓMEZ RIVERO, M.C. (2012) «*Los delitos contra la propiedad intelectual e industrial*». Ed. Tirant lo Blanch. Valencia.

GONZÁLEZ CUSSAC, J.L. Y LARRIBA HINOJAR, B. (2011) «*Inteligencia económica y competitiva*». Ed. Tirant lo Blanch. Valencia.

HERRERA HERMOSILLA, J.C. (2012) «*Breve historia del espionaje*». Ed. Nowtilus. Madrid.

IZQUIERDO TRIANA, H. (2016) «*Inteligencia competitiva*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 215-221. Ed. Tirant lo Blanch. Valencia.

JUILLET, A. (2006) «*Principios y aplicación de la Inteligencia Económica*». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º. 1, pp. 113-135. Madrid.

LARREINA GARCÍA, S. (2016) «*Vigilancia tecnológica*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 383-389. Ed. Tirant lo Blanch. Valencia.

Ley 3/1991, de 10 de enero, de Competencia desleal. BOE núm. 10, de 11/01/1991.

Ley Orgánica 10/1991, de 23 de noviembre, del Código Penal. BOE núm. 281, de 24/11/1995.

LOWENTHAL, M. (2006) «*Intelligence: From Secrets to Policy*». CQ Press. Washington D.C.

MARTÍNEZ-BUJÁN PÉREZ, C. (2010) «*Delitos relativos al secreto de empresa*». Ed. Tirant lo Blanch. Valencia.

MARTÍNEZ LAÍNEZ, F. (2016) «*Espionaje*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 141-147. Ed. Tirant lo Blanch. Valencia.

MORANT, J. Y LÓPEZ, A. (coord.) (2013) «*Detección de APTs*». Centro de Seguridad TIC de la Comunitat Valenciana

(CSIRT-CV). Instituto Nacional de Tecnologías de la Comunicación (INTECO) (actual INCIBE-Instituto Nacional de Ciberseguridad).

NAVARRO BONILLA, D. (2014) «*Espionaje*». En, De la Corte Ibáñez, L. y Blanco Navarro, J.M. (coord.) «*Seguridad Nacional, amenazas y respuestas*». LID Editorial. Madrid.

OLIER ARENAS, E. (2013) «*La inteligencia económica en un mundo globalizado*». Cuaderno de Estrategia, n.º 162. Instituto Español de Estudios Estratégicos. Madrid.

OLIER ARENAS, E. (2016) «*Inteligencia económica*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 233-240. Ed. Tirant lo Blanch. Valencia.

ORTS BERENGUER, E. Y GONZÁLEZ CUSSAC, J.L. (2004) «*Compendio de derecho penal (parte general y parte especial)*». Ed. Tirant lo Blanch. Valencia.

PRIETO DEL VAL, T. F. (2016) «*Espía*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 133-140. Ed. Tirant lo Blanch. Valencia.

PRUNCKUN, H. (2012) «*Counterintelligence: Theory and Practice*». Ed. Rowman & Littlefield. Lanham.

REGO FERNÁNDEZ, M. (2016) «*INFOSEC (Information Security)*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 207-213. Ed. Tirant lo Blanch. Valencia.

RUIZ RODRÍGUEZ, L. R. (2016) «*Espionaje industrial*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 149-156. Ed. Tirant lo Blanch. Valencia.

TEJADA DE LA FUENTE, E. Y MARTÍN MARTÍN DE LA ESCALERA A.M. (2016) «*Ciberdelitos*». En, Díaz Fernández, A.M. (dir.) «*Conceptos fundamentales de inteligencia*», pp. 37-44. Ed. Tirant lo Blanch. Valencia.

WETTERING, F.L. (2000) «*Counterintelligence: The Broken Triad*». *International Journal of Intelligence and Counterintelligence*, n.º 13 pp. 265-300. Routledge. Abingdon-on-Thames.