NOTAS SOBRE LA DELINCUENCIA INFORMÁTICA: ATENTADOS CONTRA LA "INFORMACIÓN" COMO VALOR ECONÓMICO DE EMPRESA

Mariluz Gutiérrez Francés

Profesora de Derecho Penal. Universidad de Salamanca

Estudios de Derecho penal económico. Ediciones de la Universidad de la Universidad de Castilla – La Mancha (Estudios; 18), Cuenca, 1994

NOTAS SOBRE LA DELINCUENCIA INFORMÁTICA: ATENTADOS CONTRA LA "INFORMACIÓN" COMO VALOR ECONÓMICO DE EMPRESA

MARILUZ GUTIÉRREZ FRANCÉS
Profesora de Derecho Penal
Universidad de Salamanca

1. INTRODUCCION

Vivimos en plena "era de la informatica". Las sofisticadas calculadoras electrónicas, funcionales, fiables y de gran capacidad, han invadido los ámbitos más diversos de las relaciones socioeconómicas. pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por el ordenador directa o indirectamente. Sectores como la banca, los seguros, los transportes, la educación, la bolsa, el tráfico aéreo y terrestre, las Administraciones Públicas en su conjunto..., dependen, en gran medida, de las computadoras. A ellas se les encomienda, ya no sólo el archivo y procesamiento de información sino, incluso, la adopción automática de decisiones, por lo que se han convertido en "el caballo de trabajo del siglo XX", o "el genio mágico" —en palabras de BEQUAI[1]—.

Desde la segunda guerra mundial y, sobre todo, desde la introducción del microprocesador en 1975, el ordenador ha desbordado su marco estilista inicial (el de las grandes multinacionales), invadiendo todo tipo de negocios y empresas, oficinas y escritorios

[1] BEQUAI, A., *Computer Crime*, Heath Lexington Books, Lexintong, 1978, p. XIII.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

privados. La miniaturización de los *computer chips*, el incremento de la capacidad de almacenamiento y procesamiento de datos, el desarrollo de la telemática (por la fusión del procesamiento de información y las nuevas tecnologías de la comunicación), así como la investigación en el campo de la inteligencia artificial, han favorecido la difusión y popularización de los ordenadores, generando una *computer dependency* en la que todas las sociedades modernas están involucradas.

La revolución informática ha incidido de forma insospechada en el viejo concepto de "la información", revitalizándolo espectacularmente e incrementando de forma extraordinaria su valor. Las nuevas técnicas posibilitan una potenciación indefinida de las acumulaciones de datos en poco espacio, de fácil acceso y recuperación, a través de una clave o código único, en cuestión de escasos segundos y de también muy simple interrelación, tratamiento y transmisión. Como consecuencia, lo que tradicionalmente hubiera constituido una mera acumulación de datos, hoy, a causa del impacto de la revolución informática, se ha transformado en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico.

Este fenómeno, ciertamente, tiene lugar en toda sociedad —y en cada parcela— donde ha irrumpido de forma espectacular la informática[2]. Sin embargo, si tuviéramos que destacar algún sector particularmente afectado por el impacto de las nuevas tecnologías, señalaríamos, sin duda, el mundo de la empresa. No es posible ignorar el rápido proceso de informatización que se ha producido a nivel industrial y comercial en las últimas décadas, al que también se ha unido España como en una frenética carrera. Pequeñas y grandes empresas, multinacionales y compañías de toda índole, han descubierto en los modernos sistemas de proceso de datos un valioso y útil instrumento que facilita y potencia su actividad económica y que representa una notable ventaja competitiva en el mercado.

Y, desde luego, si en algún sector la revolución informática ha revitalizado este viejo concepto de la información, hasta despuntar como un bien autónomo valioso, objeto del tráfico a precios de mercado muy elevados, éste es, precisamente, el sector que ahora nos ocupa: el de la actividad empresarial e industrial. Hoy la informatización implica a las contabilidades de empresas, carteras de clientes, balances, informes y proyectos empresariales, estrategias de mercado, procedimientos económicos o tecnológicos de carácter reservado, así como datos de investigación y desarrollo de la tecnología. Pues bien: las peculiares características de los sistemas informáticos y de su funcionamiento, la todavía notable desprotección material y logística de las bases de datos informatizados —pese al avance producido en sistemas para criptografiar y codificar información— y la importancia que para el tráfico económico empresarial poseen los programas y la información almacenada en soportes informáticos, hacen de ésta, una parcela especialmente vulnerable ante conductas lícitas de diversa índole (contrapunto de las ventajas que el uso de los sistemas de proceso automático de datos comporta). Consideremos, a título de ejemplo, el siguiente supuesto:

---

[2] Sobre el impacto multidimensional de la revolución informática, vid. PEREZ LUÑO, A-E., *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información,* Fundesco, Madrid, 1987, pp. 34-37.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

Madrid, 2 de julio de 1993: La Compañía "Alfa-Beta Soluciones Microinformáticas" se querella ante el Juzgado de Instrucción Número 20 de Madrid contra su equipo de *software*, a quienes acusa de apropiación indebida de material informático por valor de 700 millones de pesetas, y de sabotaje por importe de otros 500 millones de pesetas. Sólo veinticuatro horas antes, los empleados de dicha Compañía habían demandado a la misma ante la Magistratura de Trabajo por el impago de los salarios de varios meses y en solicitud de resolución de contrato. Cuatro de los técnicos denunciados fueron detenidos en su domicilio, llegando a ingresar uno de ellos en prisión preventiva en la cárcel de Carabanchel durante algunos días[3].

(Fuentes de la misma Compañía informan que dichos empleados han abandonado la empresa, llevándose material informático de titularidad de Alfa-Beta y dejando codificados y encriptados —es decir, inutilizables— los sistemas y el material informático de la misma, y han constituido otra empresa de la competencia.

A falta de más datos para evaluar un hecho tan reciente, aún en fase de investigación, sirva a estas líneas por las reflexiones e interrogantes que sugiere y que nos introducen, directamente, en el objeto de nuestra investigación. A tenor de lo que destaca esta breve nota de prensa, pudiéramos estar ante uno o varios lícitos informáticos, *ocurrido dentro de nuestras fronteras* (lo que constituye una novedad, porque hasta hace muy pocos años, supuestos de estas características sólo eran imaginables en contextos con un nivel de desarrollo económico y tecnológico muy superior al nuestro). En la actualidad, nadie discute que España se ha incorporado a las ventajas que reporta la "era de la informática", pero también a sus riesgos, a su dimensión pervertida[4]. Por otra parte, el caso así expuesto, nos plantea numerosos interrogantes: ¿Cabría tomar en consideración las figuras tradicionales de apoderamiento material para la obtención ilícita de *software*? ¿Que relevancia tiene, en orden a la calificación jurídica de los hechos, la pertenencia de los sujetos denunciados al equipo técnico de la empresa, es decir, la existencia de una relación de dependencia laboral, y la posterior ruptura unilateral de la misma? ¿Subsiste, a la ruptura de dicha relación, el deber de guardar secreto, incluso en relación con el soporte lógico que los propios técnicos contribuyeron a crear durante su vinculación laboral a la empresa denunciante? ¿Cabría hablar de espionaje informático si la nueva empresa constituida se aprovecha de la cartera de clientes de la víctima? ¿Constituyen los actos de codificación y encriptación de información un supuesto de sabotaje informático? ¿De que instrumentos dispone nuestro Derecho positivo frente a este tipo de conductas que atentan contra la información como valor económico de empresa? A la espera de un nuevo Código Penal, y con el Proyecto de 1992 en la mano, ¿Que cauces incorpora a tal efecto —o debiera incorporar—?

Todos estos interrogantes nos conducen, sin más dilación, al objeto de nuestro estudio: a partir de ahora vamos a ocuparnos de la "información" (almacenada, tratada y transmitida mediante los sistemas de procesamiento de datos), como valor económico de empresa[5] que confiere a su titular una posición ventajosa en las relaciones del tráfico eco-

---

[3] PCWEEK, 22 de julio de 1993.

[4] Vid. por todos, CAMACHO LOSA, L., *El delito informático*, Madrid, 1987, *passim*. ROMEO CASABONA, C.M., *Poder Informático y seguridad Jurídica,* Fundesco, Madrid, 1987, p. 37.

[5] Vid. ROMEO CASABONA, C.M., *Poder Informático...*, cit., pp. 168-170. "Computer Crimes and Other Crimes Against Information Technology in Canada", *International Review of Penal Law*, "AIDP", vol. 64, 1993, pp. 210-211.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

nómico. Como interés social valioso digno de la tutela penal, nos acercaremos a las vías insaturadas por nuestro Derecho punitivo para su protección, frente a los comportamientos ilícitos que más gravemente pueden atacarlo, conductas susceptibles de engrosar alguna de estas tres grandes categorías: a) El espionaje informático industrial o comercial; b) Las conductas de daños o sabotaje informático; y c) Las conductas de mero intrusismo, también conocidas por el término anglosajón "*hacking*".

Como tendremos ocasión de comprobar, las fronteras entre estas grandes categorías no son siempre nítidas. La dinámica comisiva de esta clase de ilícitos propicia las situaciones concursales. Así, no será infrecuente que un comportamiento de espionaje empresarial vaya acompañado de una modificación o destrucción de datos, submisible 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. (Situaciones como las indicadas, nada tienen de fantasía, como demuestran algunos hechos que suministra la experiencia en otros países: Recuérdese, en los Estados Unidos, el caso del joven de diecisiete años que en 1985 se infiltró, desde su ordenador personal, con la ayuda de un *modem* y un teléfono, en los sistemas informáticos del Pentágono, provocando la modificación de valiosos datos informatizados sobre construcción de material de defensa y ubicación de satélites artificiales en el espacio[6]. O dentro del mismo contexto, el "caso Morris": un joven que interfirió los sistemas informáticos del Ministerio de Defensa, infectando con un "virus" más de seis mil computadoras oficiales que contenían valiosos archivos y ficheros de información clasificada)[7]. En consecuencia, será la dimensión subjetiva de la conducta la que, con frecuencia, nos aporte el criterio delimitador en cada caso.

2. ESPIONAJE INFORMATICO INDUSTRIAL O COMERCIAL

Frente al planteamiento doctrinal más extendido, dentro y fuera de nuestras fronteras, consideramos imprescindible la adjetivación del concepto "espionaje informático" con las referencias a lo "industrial" y "comercial" (empresarial)[8]. Pues, de no ser así, habríamos de incluir, junto a éste, otras modalidades de espionaje informático que inciden en bienes jurídicos de muy distinta naturaleza, como la seguridad interior o exterior del Estado, la defensa nacional, etc. Hecha esta advertencia, urge delimitar las conductas a que nos estamos refiriendo: Se viene entendiendo por espionaje informático (añadiríamos los adjetivos "comercial" o "industrial") la obtención, como ánimo de lucro y sin autori-

[6] MARBRACH, W.D., KASINDORF, M., SANDZA, R., "Was It Really War Games?", *Newsweek*, vol. 106, 1985, p. 23.

[7] Publicado en EL PAIS, 10 de enero de 1990, p. 26.

[8] Por todos, SIEBER, U., *The International Handbook on Computer Crime* John Wiley and Sons, Chichester, 1986, pp. 12 y ss.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

además, "de valor para el tráfico económico de la industria o comercio").

Señala ROMEO CASABONA[10] que, desde el punto de vista jurídico, el tratamiento penal del espionaje informático encierra problemas mayores que otras parcelas de la criminalidad informática, incluidos los fraudes informáticos. Y no le falta razón, a la vista del complejo elenco de conductas que tienen cabida en este apartado: apoderamiento, obtención, copia o memoración de ficheros de datos relativos a patentes de invención, modelos de utilidad, dibujos y modelos industriales, marcas de fábrica o de comercio, nombres comerciales, indicaciones de procedencia y denominaciones de origen (materias que nos colocan en el área de los derechos de la propiedad industrial), obtención o copia de ficheros que recojan una obra literaria, artística o científica, en el sentido amplio de la Ley de Propiedad Intelectual, copia, obtención y/o destrucción de datos informatizados sobre informes financieros, carteras de clientes, estudios de mercado, estrategias empresariales, contabilidades y balances, etc., tengan o no carácter reservado.

No existe, en punto al espionaje informático empresarial, una regulación específica en nuestro Derecho positivo vigente, a diferencia de otras legislaciones próximas, como la alemana, austríaca, griega, etc.[11]. Se aparta así nuestro ordenamiento de las recomendaciones de la comunidad internacional, desde las distintas instancias, de procurar armonización legislativa en la materia[12]. De esta suerte, tenderemos que poner a prueba las distintas vías que continúa ofreciendo el Derecho tradicional, cuyas posibilidades, como veremos, son bastantes limitadas.

2.1. Cauces para el espionaje informático empresarial en el Derecho vigente

Como punto de partida se debe rechazar, con el planteamiento doctrinal más extendido, la aplicabilidad de las figuras de apoderamiento material a los supuestos de copia u obtención de ficheros informáticos con ánimo de lucro y sin autorización: no estamos aquí ante "cosas muebles, corporales, tangibles", sino que la acción recae sobre elementos inmateriales, intangibles, no susceptibles de apoderamiento material. (No se debe olvidar, como bien recuerda GONZALEZ RUS[13] "que los elementos lógicos (*software*, ficheros) no son, sino un conjunto de información al que se accede eléctricamente. Unas veces, en

---

[9] ROMEO CASABONA, C.M., "*Delitos patrimoniales en conexión con sistemas informáticos y de telecomunicación*", *Textos de ponencias y comunicaciones.* Congreso sobre Derecho Informático, Facultad de Derecho de Zaragoza, Zaragoza, 1989, p. 512, en la línea de SIEBER, ult. cit. GONZALEZ RUS, J.J., en *Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, "Poder Judicial", nº especial IX, CGPJ, Madrid, 1989, p. 42, incorpora la nota del "ánimo de lucro", a nuestro juicio, acertadamente.

[10] ROMEO CASABONA, ult. cit., p. 512.

[11] En Alemania, cfr. MÖHRENSCHLAGER, M., *Computer Crimes and Other Crimes Against Information Technology in Germany*, "International Review of Penal Law", "AAIDP", vol. 64, pp. 344 y ss.; VASSILAKI, I., *Computer Crimes and Other Crimes against Information Technology in Greece*, "International Review...", ult. cit., pp. 361 y ss.; la situación legislativa en Austria, desde la reforma de 1987, en SCHICK, P.J., SCHMÖLZER, G., *Computer Crimes and Other Crimes against Information Tehnology in Austria*, "International Review...", ult. cit., pp. 141 y ss.

[12] Una revisión al tratamiento del espionaje en las distintas legislaciones nacionales en, SIEBER, U., *The International Emergence of Criminal Information Law*, Carl Heymanns Verlag KG., Köln, 1992, pp. 18 y ss., y las actuaciones para la armonización legislativa, *ibidem*, pp. 76 y 22.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

la memoria central del ordenador, a la que se llaman los programas o ficheros para procesarlos; otras, en memorias auxiliares en las que se graba magnéticamente el programa o el fichero con vistas a su utilización futura".) Los elementos lógicos constituyen, pues, una especie de "flujo electromagnético", no subsumible en el concepto de "cosa mueble" de los delitos de apoderamiento —como tampoco se incluyen en dicho concepto otras energías, lo que se deduce de la opción legislativa de incorporar al Código los artículos 536 y siguientes—. Esta misma limitación se observa en todos los ordenamientos jurídicos tradicionales, cuyas figuras de apoderamiento están concebidas para la protección de la propiedad de cosas corporales, aprehensibles, susceptibles de desplazamiento, característica que no puede predicarse de los elementos lógicos de los sistemas informáticos. Por ésta razón, la adaptación legislativa a la nueva realidad que nos ocupa ha consistido, en algunos países, en la reinterpretación del concepto de "propiedad" a los efectos de los delitos de apoderamiento, a fin de incluir también los intangibles[14].

En segundo lugar, el recurso a las disposiciones —civiles y/o penales— protectoras de la propiedad intelectual, aunque posible, es también una opción bastante limitada: más allá de la protección de los programas frente a lo que se conoce como "piratería de *software*" (conductas de copia o reproducción, sin autorización del titular, y con ánimo de comercialización ilícita, objeto de un análisis diferenciado en atención a su dinámica comisiva),[15] sólo cabrá la aplicación de tal legislación a los supuestos en los que el contenido de los ficheros y bancos de datos informatizados afectados por las conductas de espionaje tenga, ya antes de su incorporación al soporte informático, la consideración de obra o creación "original", "científica, artística o literaria", y siempre, claro está, que no posea el carácter de "secreto"[16]. Y si ya es discutible que los archivos informatizados (sobre carteras de clientes, balances, recopilaciones de direcciones, etc.) puedan ser calificados de "creación original, científica, artística o literaria", mayores dificultades planteará la última de las exigencias mencionadas: por lo general, las bases de datos y ficheros empresariales conservan su valor y operatividad en tanto son de conocimiento reservado, mien-

---

[13] GONZALEZ RUS, *Tratamiento penal de los ilícitos patrimoniales...*, cit., p. 43.

[14] Así, por ejemplo, en los Estados Unidos; sobre la reinterpretación del delito federal de "transporte interestatal de mercancías robadas" y otros delitos de carácter estatal (local), vid. en, GUTIERREZ FRANCES, M., *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, pp. 145-146; cfr. también el concepto amplio de "propiedad" del artículo 2 del C.P. canadiense, o los artículos 1 y 4 (1) de la Theft Act de 1968 (Reino Unido), que engloban en la propiedad los "intangibles".

[15] Respecto a la protección de programas frente a la llamada "piratería de *software*", se habrá de acudir, en sede civil, a la Ley de Propiedad Intelectual, de 11 de noviembre de 1987, particularmente al régimen jurídico especial que para los programas establecen los artículos 96 y siguientes de dicha Ley, régimen parcialmente modificado por l Ley 16/1993, de 23 de diciembre, que incorpora al Derecho español la Directiva 91/250 del Consejo de la CEE, de 14 de mayo de 1991, sobre protección jurídica de los programas de ordenador. Y, en sede penal, punto de referencia obligado lo constituyen los artículos 534 bis a) y siguientes del C.P., introducidos por la reforma penal de 11 de noviembre de 1987, donde se abandona, al menos formalmente, la técnica de la "ley penal en blanco".

[16] El que la LPI, en su artículo 20.2 h) considere un acto de comunicación pública el acceso público a bases de datos de ordenador por medio de telecomunicación, cuando estas constituyan o incorporen obras protegidas por dicha Ley, nos ratifica en nuestro planteamiento: dichas obras tiene que ser ya antes de su incorporación al soporte informático objeto de protección por la LPI. Coincidimos, pues, con la postura defendida por ROMEO CASABONA, *Poder Informático...*, cit., p. 171.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

"creación original, científica, artística o literaria", mayores dificultades planteará la última de las exigencias mencionadas: por lo general, las bases de datos y ficheros empresariales conservan su valor y operatividad en tanto son de conocimiento reservado, mientras suponen una ventaja competitiva (de hecho, normalmente dejará de tener interés dicha información si llega al conocimiento público).

Como vía alternativa para reprimir las conductas de espionaje informático empresarial, intentamos, a continuación, los delitos de descubrimiento y revelación de secretos. Y eso nos remite a los artículos 497 y siguientes del C.P., en un Capítulo conflictivo que aúna atentados a bienes jurídicos de naturaleza diversa, e integrado en un Título complejo y hetereogéneo —y no menos conflictivo—, "De los delitos contra la libertad y seguridad". Pues bien, basta un rápido repaso por los preceptos citados para comprobar lo insatisfactorio de esta opción, confirmándonos en la idea de que ésta es una de las parcelas de nuestro Código donde la reforma se está demandando con mayor urgencia:

El artículo 497 del C.P. tipifica la conducta de quien, para descubrir los secretos de otro, se apodera de sus papeles o cartas y divulga aquéllos, imponiendo menor pena para el caso en que no se divulguen los mismos[17]. Nadie cuestiona que se trata de una figura orientada a la protección del bien jurídico "intimidad personal", con lo cual, fácilmente se deduce que sus posibilidades para castigar los supuestos de copia de elementos lógicos de los sistemas informáticos económicamente valuables y con ánimo de lucro son más bien escasas. Ya por razón del bien jurídico, *debieran*[18] quedar excluídos todos los casos en que el descubrimiento de la información contenida en los ficheros no afecte a la intimidad de su titular. (Con todo, cabría una interpretación forzada orientada a encauzar por esta vía conductas de apoderamiento de secretos industriales, habida cuenta de que no hay ninguna referencia en la descripción típica al bien jurídico intimidad, y el contenido del secreto se halla delimitado en el texto). Pero, además, el ámbito del precepto se circunscribe a los "secretos" (información reservada que el titular quiere mantener oculta) contenidos en "cartas o papeles"; luego, no es aplicable al acceso a ficheros informáticos para la obtención o copia de información, tenga esta o no el carácter de secreto. Así pues, la restricción de la tutela a los secretos documentales dejaría sólo abierta la posibilidad de aplicar esta figura —caso de superarse los problemas de bien jurídico— a los supuestos en los que la información reservada hubiera sido objeto de impresión en un "papel". Finalmente, el elemento subjetivo "animo de obtener una ventaja competitiva con valor económico y en perjuicio de otro" que preside el espionaje industrial por medios informáticos, no queda cubierto en este delito (en tal sentido, apunta GONZALEZ RUS[19] que

---

[17] Para un examen de esta figura, vid. MORALES PRATS, F., *La Tutela penal de la intimidad: "Privacy" e informática*, Destino, Barcelona, 1984, pp. 176-197, donde se ocupa de enjuiciar críticamente la técnica legislativa empleada y lo anacrónico de su configuración, lo que convierte al artículo 497 en un cauce insuficiente para la protección de los secretos (personales) documentales.

[18] Subrayamos "debieran" porque, atendiendo sólo al propio tenor del precepto, nada impedirá su aplicación para la tutela de secretos de otra índole, sean industriales o empresariales, de Estado, información secreta de las administraciones públicas, etc. En tal sentido, apunta MUÑOZ CONDE, en *Derecho Penal.* P.E., 9ª ed., Tirant lo Blanch, Valencia, 1993, p. 157, que es irrelevante que el secreto sea de carácter público o privado.

[19] GONZALEZ RUS, *Tratamiento penal de los ilícitos patrimoniales...*, cit. p. 45.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

los apoderamientos inspirados exclusivamente en el ánimo de lucro deben ser excluídos del precepto: el elemento subjetivo del injusto *apoderarse para descubrir los secretos,* no permite subsumir los que se hagan exclusivamente con *ánimo de lucro*).

Por su parte, el artículo 498 castiga con arresto mayor y multa al administrador, dependiente o criado que en tal concepto supiere los secretos de su principal y los divulgares. Tradicionalmente, esta figura se ha venido interpretando como un instrumento para la protección de la intimidad, como el artículo 497 ya citado, frente al artículo 499, orientado a la protección del secreto industrial[20]. Mas, el que nuestra jurisprudencia venga considerando estos preceptos como intercambiables[21], unido a la formulación típica del artículo 498 —que, como el artículo 499, responde a una dinámica bien distinta a la del artículo 497, al ser irrelevante el soporte al que se incorpora el secreto y que su divulgación se haga con ánimo de lucro—, abre las posibilidades de esta figura en el ámbito que nos ocupa. En cualquier caso, su virtualidad siempre estará limitada: por razón del sujeto activo ("administrador, dependiente o criado", dice el artículo 498, es decir, persona que, en relación de dependencia o subordinación, desarrolla funciones por cuenta ajena, en virtud de las cuales surge el deber de sigilo respecto a los secretos del principal); por razón del objeto material del delito ("secretos"); y por la modalidad de conducta descrita (es necesario que los secretos se "divulguen", con lo cual, la acción típica no abarca el apoderamiento. El sujeto activo tiene que hallarse en situación de conocimiento ilícito del secreto, pues, en caso contrario, como apunta GONZALEZ RUS, será preferente el artículo 497.[22] En suma, no obstante las reticencias que plantearía el recurso a esta figura por razón del bien jurídico, y como quiera que en tal cuestión la formulación típica es ambigua, podemos concluir admitiendo cierta virtualidad del tipo del artículo 498 en relación con el espionaje informático empresarial).

El artículo 499, por el contrario, a pesar de su criticable incardinación sistemática, si parece, *a priori,* dotado de una mayor aptitud para reprimir los supuestos de espionaje industrial informático, al erigirse en el instrumento único que arbitra nuestro Derecho positivo vigente para proteger penalmente el secreto industrial o comercial. El artículo 499 castiga con arresto mayor y multa al encargado, empleado u otro obrero de una fábrica u otro establecimiento industrial que, en perjuicio del dueño, descubriere los secretos de su industria[23].

Las posibilidades de aplicar esta figura a las conductas que nos ocupan se ve favorecida por algunos de los rasgos de su descripción típica. Así por razón del bien jurídico, la doctrina más extendida entiende que aquí se procura la protección de la capacidad com-

---

[20] Así, por ejemplo, BAJO FERNANDEZ, en *Derecho Penal Económico. Aplicado a la actividad empresarial*, Civitas, Madrid, 1978, pp. 278 y ss., sólo se ocupa del artículo 499 como instrumento de protección penal del secreto industrial.

[21] Vid. el comentario al planteamiento del Tribunal Supremo en, BAJO FERNANDEZ, M., *Manual de Derecho Penal*, P.E., vol. II, 2ª ed., Centro de Estudios Ramón Areces, Madrid, 1993, p. 377.

[22] GONZALEZ RUS, *Tratamiento penal de los ilícitos patrimoniales...*, cit. p. 45; en el mismo sentido, MORALES PRATS, *La tutela penal de la intimidad...*, cit., p. 203.

[23] Vid., por todos, BAJO FERNANDEZ, *Derecho Penal Económico...*, cit., pp. 277 y ss.; el mismo autor, *El secreto profesional en el Proyecto de Código Penal*, "ADPCP", 1980, pp. 595 y ss.; GOMEZ SEGADE, J.A., *El secreto industrial*, Madrid, 1974; JORGE BARREIRO, A., *Descubrimiento y revelación de secretos. Un estudio de Derecho Penal español*, "RPD", nº 87, 1982, pp. 249 y ss.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

petitiva de la empresa en el mercado (el bien que resulta afectado por el espionaje informático empresarial). Se castiga el hecho de "descubrir", entendiendo como "revelar", el secreto. Pero, ni le exige que el sujeto activo comprenda el contenido de lo que revela, ni la consumación precisa de la producción efectiva de un perjuicio económico estimable, cuantificable.[24] No habiendo delimitado el legislador el elenco de conductas típicas, es posible su aplicación a los supuestos de copia de ficheros o archivos informatizados, o a los supuestos de simple visualización en pantalla y memorización de la información, con la posterior revelación a otro u otros. Del tenor del artículo 499 no se desprende que el actor deba tener acceso al secreto por un cauce lícito, de modo que cabe subsumir los supuestos en los que obtiene subrepticiamente los datos o ficheros informatizados y los transmite.

Sin embargo, las limitaciones de su virtualidad respecto a los casos de espionaje informático devienen, de una parte, del objeto material del delito (la información de carácter empresarial o comercial ha de ser "secreta", cualquiera que sea el soporte en que haya sido incorporada), y, de otra, del círculo de posibles sujetos activos (se trata de un delito especial, que solo puede ser cometido por el "encargado, empleado u obrero" del establecimiento industrial o fábrica, es decir, aquel que, en el momento de la comisión del delito, !se encuentra bajo una relación de dependencia con el principal en condiciones que implican un depósito de confianza"[25]. Quedan excluídos, en definitiva, los comportamientos de espionaje informático realizados por terceros, lo cual, dadas las posibilidades que ofrecen las nuevas tecnologías de penetrar en un sistema informático a distancia, constituye una grave laguna. Tampoco puede reprimirse la conducta del empleado que conoce cualquier cauce, lícito o ilícito, la información secreta y, en lugar de revelarla —descubrirla— a otro, la utiliza personalmente para constituir su propia empresa, haciendo la competencia desleal a la víctima (sólo cabría aquí, en su caso, la aplicación de la Ley de Competencia Desleal)[26]. Adicionalmente, la presencia del elemento subjetivo del injusto (intención de perjudicar a la empresa o industria) excluye la posibilidad de castigar la actuación culposa. Es decir, no es aplicable, por ejemplo, a los supuestos en los que la actuación negligente o poco cuidadosa en la custodia y tratamientos de ficheros y bancos de datos informatizados secretos, provoca el descubrimiento de la información valiosa por terceros. (Los estudios criminológicos sobre delincuencia de casos, la actuación ilícita estuvo favorecida, cuando no provocada, por la negligencia de empleados y responsables de los equipos informáticos)[27], En suma, se trata de una solución insuficiente e insatis-

---

[24] Cfr. BAJO FERNANDEZ, *Manual de Derecho Penal*, P.E., vol. II, 2ª ed., cit., p. 382.

[25] JORGE BARREIRO, *Descubrimiento y revelación...*, cit., pp. 253.

[26] No existe acuerdo en la doctrina sobre este punto ya que, si como parece que exige el tipo, debe existir la relación de dependencia o subordinación laboral al tiempo de revelarse el secreto, fácilmente podría eludirse la realización del delito con la sola ruptura voluntaria de la relación laboral, por parte del empleado, justo antes de llevar a cabo la conducta prohibida. Sin embargo, el tenor del precepto parece que no admite discusión, y la solución para estos casos, parece que sólo puede ser la represión extrapenal del hecho, a través de la citada Ley de Competencia Desleal, (particularmente, por el cauce de los artículos 13 y 14). Vid. GOMEZ SEGADE, *El secreto industrial* cit., pp., 377 y ss.

[27] Encontramos entre la casuística americana el supuesto de una empresa multinacional de equipos informáticos que, en los libros de instrucciones que entregaba a loa adquirientes de los ordenadores, incluía, a título de ejemplo, por error, el código de acceso secreto al propio sistema informático de la compañía. Con lo cual, las conductas de *hacking* habían sido frecuentes, y propiciadas por un error de la propia víctima. Vid. en, GUTIERREZ RANCES, *Fraude informático...*, cit., pp. 66-67.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

factoria para la problemática que hoy representa, en las sociedades modernas, el espionaje industrial —informático y no informático—.

El artículo 497 bis, incorporado al C.P., junto con el artículo 192 bis, por Ley Orgánica 7/1984, de 15 de octubre, con el fin de reprimir la interceptación de las comunicaciones telefónicas y la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido, *podría* también dar algún juego en el ámbito del espionaje informático. Presenta, de partida, las mismas restricciones que el artículo 497 en atención al bien jurídico, ya que, según la interpretación más extendida de esta figura, tiende a la protección de la intimidad de las comunicaciones personales orales[28]. Sin embargo, forzando una determinada lectura —de la fórmula disyuntiva "secretos o intimidad"—, podría admitirse un concepto amplio del "secreto", comprensivo también del secreto industrial o comercial. superado este obstáculo, ya no veríamos problemas para castigar por esta vía, por ejemplo, supuestos en los que se intercepta la información reservada en la fase de transmisión electrónica de datos de una terminal a otra, o aquellos en los que se instalan los artificios técnicos para interferir o reproducir tal información[29].

Respecto a ficheros o bancos de datos informatizados que posean el carácter de reservado o secreto, aún cabe el recurso a la normativa que se ocupa de la protección de la competencia:

Anteriormente, la represión de las conductas de competencia desleal se llevaba a cabo dentro de la Ley de Propiedad Industrial de 1902. En la actualidad, debemos acudir a la Ley 3/1991, de 10 de enero, de Competencia Desleal[30], con la que el legislador ha pretendido superar modelos de regulación desfasados y sin parangón alguno en Derecho comparado. Se trata, desde luego, de una regulación extrapenal (no hay delito de competencia desleal en Derecho vigente, como tampoco se tipifica en el Proyecto de 1992, a diferencia de los Proyectos anteriores, que sí recogían tal delito), pero debemos referirnos a ella en estas lineas por las previsiones que directamente se ocupan de la violación de secretos empresariales).

El artículo 13.1 dispone 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 haya tenido acceso, legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente (referido a la adquisición de secretos mediante espionaje o procedimiento análogo), o

---

[28] Vid. MORALES PRATS, *Problemática jurídico-penal de las libertades informáticas en España tras diez años de vigencia de la Constitución de 1978*, Separata de "Estudios Penales y Criminológicos", nº XII, Universidad de Santiago de Compostela, 1989, p. 361; GONZALEZ GUITIAN, L., *Protección penal de la intimidad y escuchas clandestinas*, en *Comentarios a la legislación penal*, (COBO DEL ROSAL-BAJO FERNANDEZ), T.VII, Edersa, Madrid, 1986, pp. 49 y ss.; Vid. también en, MUÑOZ CONDE, *Derecho penal*, P.E., 9ª ed., cit., p. 160, donde señala como objeto de protección "la intimidad de las comunicaciones personales orales". El mismo autor, para una extensa relación bibliográfica sobre este delito.

[29] Vid. MORALES PRATS, *Problemática jurídico-penal...*, cit. p. 362, rechazando la aplicabilidad del artículo 497 bis para los supuestos en que se interfiere una transmisión informática de datos.

[30] Sobre la Ley de Competencia Desleal, vid. OTERO LASTRES, J.M., *La nueva ley sobre Competencia Desleal*, "La Ley", año XII, nº 28.55, 17 de octubre de 1991. Para el estudio desde la perspectiva del Derecho Comunitario, TIEDEMANN, K., *Lecciones de Derecho Penal Económico, (comunitario, español y alemán)*, PPU, Barcelona, 1993, pp. 57 y ss.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

en el artículo 14 (que se refiere a las conductas de inducción da un trabajador, proveedor, etc., a romper las obligaciones contractuales contraídas con los competidores). El párrafo tercero del mismo artículo establece, en casos de violación de secretos, una excepción al régimen general del artículo 2 —que no es aplicable—. No obstante, precisa que la violación se haya efectuado con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto.

En el artículo 14, además de la conducta de inducción a una infracción contractual ya referida, en el párrafo segundo se ocupa de los casos en que se induce a la terminación regular de un contrato o se aprovecha de una infracción contractual ajena. Sólo se reputará competencia desleal "cuando, siendo conocida, tenga por objeto la difusión o explotación de un secreto industrial o empresarial o vaya acompañada de circunstancias tales como el engaño, la intención de eliminar a un competidor del mercado u otras análogas".

Por último, en el artículo 15.1 de la misma Ley se establece: "Se considera desleal prevalerse en el mercado de una ventaja competitiva adquirida mediante la infracción de las leyes. La ventaja ha de ser significativa".

Como se puede deducir de los preceptos anteriores, donde resulta irrelevante la fórmula concreta, lícita o ilícita, de acceder a los secretos con valor empresarial, la mayoría de las conductas que cabría subsumir en la categoría de "espionaje informático empresarial" podrán ser reprimidas por los cauces previstos en la Ley de Competencia Desleal (arts. 18 y siguientes), probablemente más eficaces que los cauces penales[31].

Por lo demás, si el contenido de los ficheros o archivos informatizados sobre los que recae la conducta de espionaje es uno de los derechos —registrados— de propiedad industrial (patentes de invención, modelos de utilidad, dibujos, marcas de fábrica o de comercio, nombres comerciales, indicaciones de procedencia o denominaciones de origen), cabrá la aplicación del artículo 534 C.P.; el empleo de la técnica de la ley penal en blanco en esta disposición por nuestro legislador, nos remite a la normativa extrapenal: la Ley de Propiedad Industrial, de 16 de mayo de 1902, la Ley de Patentes, de 20 de marzo 1986, la Ley de Marcas, de 12 de noviembre de 1988, y, de gran importancia en lo que a informática concierne, la Ley de Protección Jurídica de las topografías de los Productos Semiconductores, de 3 de mayo de 1988[32].

2.2. Referencia al Proyecto de C.P. de 1992 en materia de espionaje informático

Las dudas que hoy suscita el bien jurídico protegido en los delitos que aparecen bajo la rúbrica "Del descubrimiento y revelación de secretos", así como las posibilidades de aplicar los artículos 497, 497 bis y 498 a los atentados contra un bien distinto a la intimidad —como sucede en el espionaje informático empresarial—, se resuelven formal-

---

[31] El recurso al Derecho penal con carácter excepcional en esta materia, así como los problemas en relación con el principio de intervención mínima que provocaría la represión penal de las conductas de competencia desleal, en BERDUGO GOMEZ DE LA TORRE, I., *La reforma de los delitos contra la propiedad industrial*, en "Documentación jurídica", (Monográfico dedicado a la PANCP), nº 2, Ministerio de Justicia, 1983, pp. 737 y ss.

[32] Acerca del caos normativo que existe en España en relación con la propiedad industrial, vid. BAJO FERNANDEZ, *Manual de Derecho Penal*, P.E., vol. II, 2ª ed., pp. 264 y ss.

mente en el Proyecto. Se delimitan con nitidez las parcelas al regularse, por una parte, los atentados contra la intimidad y domicilio —se realicen o no por medios informáticos, y ya sean ejecutados por terceros, ya por sujetos vinculados de alguna forma a las víctimas— (arts. 198 y siguientes del Proyecto) y, por otro, los atentados contra los secretos empresariales o industriales —se hallen o no informatizados— (arts. 284 y 285 del Proyecto).

Los cauces fundamentales que ofrece el Proyecto para la represión del espionaje informático (empresarial o industrial) son: las disposiciones para la protección de la propiedad intelectual, las que tipifican los atentados contra la propiedad industrial y los preceptos que miran a la tutela de los secretos empresariales o industriales.

Desde luego, a la vista del Proyecto, continúa abierta la posibilidad de aplicar las disposiciones que protegen la propiedad intelectual. Como en el sistema actual, es imprescindible que las conductas de espionaje informático se hallen descritas en el artículo 259 del Proyecto (de contenido idéntico al actual artículo 534 bis a) y recaigan sobre un programa en el sentido de la Ley de Propiedad Intelectual, como se vio, o sobre bases de datos, archivos o registros informatizados cuyo contenido sea una de las obras protegidas por la legislación indicada.

Tampoco vemos obstáculo para aplicar, en el marco del Proyecto, las disposiciones que protegen la propiedad industrial. Para ello, el contenido de los archivos o registros informatizados ha de ser alguno de los derechos (registrados) a que se refiere la legislación extrapenal (Ley de Propiedad Industrial, Ley de Patentes, Ley de Marcas y Ley de Productos Semiconductores), y la conducta tendrá que ajustarse a alguna de las previstas por los artículos 281, 282 y 283 del Proyecto. Como principal novedad en punto a la tutela penal de la propiedad industrial, debemos destacar el esfuerzo del prelegislador, reflejado en los mencionados artículos 281, 282 y 283 del Proyecto, por abandonar la técnica de la ley penal en blanco, si bien esto no se logra plenamente: a la vista de la normativa proyectada, continuará resultando imprescindible el recurso a las leyes de contenido extrapenal, bien por expresa remisión de los nuevos tipos (el artículo 282 se remite expresamente a la legislación de marcas, y el artículo 283 a la legislación de patentes), bien por la necesidad de interpretar los elementos normativos empleados en estas figuras (en sentido parecido al sistema de incriminación de las infracciones de la propiedad intelectual y que, muy probablemente, suscitará análogo debate). Sobre este punto, reconoce la Exposición de Motivos del Proyecto: "La regulación que ahora se introduce se libera de la total sumisión a la Ley de Propiedad Industrial y aborda la definición en sede penal de las conductas que merecen la consideración de delitos contra aquel derecho. (...) la presencia de una Ley de obligada referencia para la interpretación o delimitación de la ley penal no supone que el legislador penal deba tomar el cómodo camino de la ley penal en blanco, técnica legislativa que sólo excepcionalmente puede admitirse dados los peligros que entraña para los principios de seguridad y taxatividad (...)".

Sin embargo, aún hallamos en el texto de 1992 otras dos disposiciones más directamente vinculadas a los comportamientos de espionaje informático empresarial o industrial: los artículos 284 y 285.

El artículo 284 establece, en su párrafo primero: "El que, para descubrir o revelar un secreto de empresa evaluable económicamente y que comporte ventajas competitivas, se apodere de documentos, soporte informático u otros objetos, o empleare alguno de los medios o instrumentos señalados en el artículo 198, será castigado..." (El inciso final de este primer párrafo prevé los casos en los que, adicionalmente, existe apoderamiento o

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

destrucción de los soportes informáticos, en tanto que el segundo párrafo tipifica la publicidad engañosa en perjuicio de la capacidad competitiva de otro en el mercado).

En el artículo 285 se describe del que "revelare un secreto industrial o de empresa evaluable económicamente y que comporte ventajas competitivas, estando legal o contractualmente obligado a guardar reserva". El párrafo segundo castiga con menor pena los supuestos en los que "el secreto se utilizare en provecho propio".

Sin entrar en profundidad en el examen de estos preceptos, apuntaremos algunas de las reflexiones que nos sugiere su lectura:

1º Ambos tipos aparecen incardinados dentro del capítulo destinado a "Los delitos relativos a la propiedad industrial, al mercado y a los consumidores", y entre los delitos contra el orden socioeconómico (a nuestro juicio, de forma clara, pese a la confusión a que puede inducir el Proyecto, que se ocupa, conjunta e indiferenciadamente, de los "Delitos contra el patrimonio y contra el orden socioeconómico")[33]. (Señala, no obstante, la Exposición de Motivos al llegar a este punto, que "se inicia el grupo de infracciones en las que el carácter económico prepondera sobre el patrimonial"). Así pues, aunque la conexión entre estos delitos y el actual artículo 499 es innegable, desde un punto de vista sistemático se puede hablar de un avance notable. Y la remisión del artículo 284 a "los medios o instrumentos" señalados en el artículo 198", no debe interpretarse cono un puente que liga *todavía* a unas y a otras infracciones. Más al contrario, sólo ratifica en la idea de que los artificios informáticos pueden servir de instrumento a ilícitos de muy diversa índole sin mutar, por ello, su naturaleza (y el empleo de artificios o medios informáticos puede ser una dinámica comisiva común a tales delitos, sin que por ello deban confundirse).

2º En clave de bien jurídico y, en la linea de razonamiento que aceptamos respecto al artículo 499 actual[34], debemos señalar que ambas figuras del Proyecto miran a la protección de "la capacidad competitiva de la empresa en el mercado", la capacidad competitiva que confiere el "secreto" industrial o de empresa. (Sigue valiendo la idea de secreto como conocimiento reservado a un círculo limitado de personas y oculto a otras, cuyo contenido, en este caso, lo integran las ideas, procedimientos o productos industriales que el empresario, por su valor competitivo, desea mantener oculto).

3º Si examinaremos separadamente una y otra figura para conocer sus posibilidades en la represión del espionaje informático industrial, llegamos a las siguientes conclusiones:

En relación con el artículo 284.1, el bien jurídico tutelado y el objeto material del delito suministran una importante vía de acceso a los ilícitos informáticos que ahora nos

---

[33] Esta fusión sistemática de ilícitos patrimoniales y contra el orden socioeconómico en el mismo obedece, en palabras de GARCIA VALDES, C., *El Proyecto del Nuevo Código Penal*, Tecnos, Madrid, p. 46, "a la difícil separación, en ocasiones, de las conductas societarias o privadas, no siempre de clara distinción. Frente a esta primera conclusión, una segunda se impuso, indebidamente a los miembros de la Comisión: que en 1992 no se podía salir con un Código que no mencionase los delitos económicos, propios de las sociedades avanzadas, cuyos autores <de cuello blanco> escapaban a las tradicionales tipificaciones <convencionales>. Resuelto este asunto positivamente, poco importa la unión terminológica y sistemática en un mismo Título del texto de los delitos contra el patrimonio y socioeconómicos, pues lo principal, su existencia en el Código, estaba despejado".

[34] Vid. BAJO FERNANDEZ, *Manual de Derecho penal*. P.E., V. II, 2ª ed., cit., p. 378; MUÑOZ CONDE, *Derecho Penal*. P.E., 9ª ed., pp. 158-159; GOMEZ SEGADE, *El secreto industrial*, cit. p. 370.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

ocupan. Pese a la restricción que representa la exigencia de que la información afectada tenga carácter secreto, deja claro el prelegislador que, a los efectos de la protección, resulta irrelevante el soporte al que el secreto —la información reservada— se halle incorporado. Recordamos, sin embargo, que para nuestra doctrina este punto, ya hoy, no representa problema alguno respecto al vigente artículo 499, que incluye —porque no los excluye—, los archivos y bancos de datos informatizados siempre que sean secretos.

En cuanto al sujeto activo, se superan, con acierto, las limitaciones del artículo 499, que precisamente excluye los supuestos de espionaje industrial realizados por o desde otras empresas competidoras de la víctima. El espionaje industrial se castigará, a tenor de lo previsto en el Proyecto, sea cual fuere el sujeto activo y su vinculación con la entidad afectada. (Sólo sería de aplicación el artículo 285, por razones de especialidad, si el que actúa está obligado, por ley o por contrato, a guardar la información reservada, y la "revela" —conducta que no precisa el artículo 284 para su consumación—).

Sin embargo, aún reconociendo el loro que esto supone, el precepto no resuelve todos los supuestos. Pensemos, a título de ejemplo, en el siguiente: En su constante reto personal por descubrir la "puerta falsa" de los sistemas informáticos, "A", desde su domicilio, y con ayuda de su PC, un *modem*, y el teléfono, se introduce de forma subrepticia en las bases de datos de la empresa "X", descubriendo su estrategia de mercado para el siguiente ejercicio económico. Al comprender "A" el filón que acaba de descubrir, y a fin de sacarle provecho económico, se pone en contacto con la empresa competidora de "X", la empresa "Z", y le vende la información interceptada.

Como se habrá observado, las dificultades para incriminar las conductas de "A" y de "Z" por la vía del artículo 284 propuesto, están vinculadas a la descripción de la conducta típica. Por una parte, la utilización del verbo "apoderarse" —tradicionalmente unido a los delitos de "apoderamiento material", y que precisa, por eso, el desplazamiento material de una cosa aprehensible—, daría como resultado una seria restricción: la información secreta, en principio, debiera hallarse incorporada a alguna clase de soporte, incluso informático, objeto del necesario desplazamiento material. En esta primera alternativa quedarían subsumidas en dificultad las conductas de espionaje en las que al autor se lleva el diskette donde se contuvieren los ficheros o bases de datos informatizados. Pero no tendrían cabida, por ejemplo, las copias efectuadas en consola, o a distancia por vía telefónica, supuestos que nada tienen de extraordinario en la actualidad. Para paliar, al menos parcialmente, las consecuencias de tal formulación, el propio artículo 284 nos remite a los medios o instrumentos descritos en el artículo 198. Como resultado de integrar ambos preceptos, lo prohibido se circunscribe a: 1° El *apoderamiento* de documentos, soportes informáticos u otros objetos... cuyo contenido sea el secreto de empresa; 2° El *empleo de artificios técnicos* de escucha, transmisión o grabación de sonido, imagen o cualquier otra señal de comunicación; y 3° El "*apoderamiento*" *de datos* registrados en ficheros, soportes informáticos o cualquier otro tipo de archivo o registro público o privado (siempre que cualquiera de estas conductas persiga el descubrimiento o revelación de un secreto de empresa evaluable económicamente y que comporte ventajas competitivas).

La integración del artículo 284 con los medios o instrumentos del artículo 198 abre, sin duda, el espectro de conductas de espionaje informático que, eventualmente, resultarán típicas (ej: los casos en los que se copia la información secreta en discos: o los supuestos en que es interceptada vía telefónica durante la fase de transmisión informática). Sin embargo, no vemos posibilidad de reprimir por esta vía otros hechos que pudieran ser rele-

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

vantes (ej: visualización y memorización de datos informatizados, sin "apoderamiento" alguno[35] ni empleo de los artificios de reproducción, grabación o comunicación mencionados en el artículo 198.1; descubrimiento casual de la información secreta y posterior comercialización de la misma a competidores). En resumen, nos parece advertir en la redacción del precepto —y en la del artículo 198— la inercia a seguir empleando fórmulas clásicamente acuñadas y conocidas, pero inservibles para estas nuevas conductas. Y, como hemos sugerido en otro lugar[36] la aprehensión de la criminalidad informática por el Derecho positivo, en no pocos casos, sólo se precisaría de un cambio de lenguaje jurídico. Pese a las críticas que, a nuestro juicio, merece el tipo alemán para reprimir el espionaje informático[37], (porque aúna espionaje de datos, cualquiera que sea el bien jurídico afectado, e, incluso, supuestos en que no se afecta a ningún bien valioso digno de tutela penal), pudiera haber servido como modelo la descripción que allí se hace de la conducta prohibida: "Quien sin autorización se procure a sí mismo o procure a otros datos..." Lo relevante, según esta fórmula, es la obtención de los datos, y no la forma concreta de obtenerlos. Y, comoquiera que muchas de las lagunas que presenta el Proyecto para reprimir el espionaje empresarial informático se deben a la redacción del propio artículo 198.2 al que se remite, de mantenerse esta técnica de remisión, sería conveniente una más correcta definición de las conductas prohibidas en el artículo 198.2 del Proyecto.[38]

En cuanto a la dimensión subjetiva del tipo, será imprescindible, además del solo, ese ánimo de "descubrir o revelar un secreto de empresa..." (elemento subjetivo del injusto), intención que debe presidir la conducta, aunque no se descubra o revele efectivamente nada. No resultan, pues, punibles, los descubrimientos fortuitos de secretos con empleo posterior de la información para atentar contra la capacidad competitiva de la víctima..

Finalmente, cabe resaltar que el tipo se construye como un delito de peligro (se consuma con el mero apoderamiento de los soportes, documentos, etc., o con el empleo de los artificios de reproducción, grabación, ..., que pongan en peligro la capacidad competitiva de la empresa en el mercado, independientemente de que los secretos hayan sido descubiertos y utilizados para lesionar la capacidad competitiva de la empresa o no, y al margen de que puedan o no constatarse perjuicios materiales cuantificables.

El artículo 285 se presenta como una versión remozada del artículo 499 en vigor, con algunos cambios notables: además de la nueva incardinación sistemática y de la clarificación del objeto jurídico, se emplea una fórmula más moderna y amplia para la delimitación de los eventuales sujetos activos. Ya no se exige dependencia o subordinación

---

[35] Vid. MORALES PRATS, *Problemática jurídico-penal...*, cit., pp. 359-360, donde distingue la solución para los casos en que los datos están "fuera del sistema" (cabría equiparar la captación mental al *apoderamiento)* y los casos en que los datos personales están ya "dentro del sistema", es decir, una vez que han sido informatizados (aquí, aun cuando se admitiese un concepto amplio del apoderamiento, siempre faltaría el soporte material).

[36] Vid. GUTIERREZ FRANCES, *Fraude informático...*, cit., pp., 621.

[37] Cfr. MÖHRENSCHLAGER, "Computer Crimes and...", cit., pp. 338 y ss.

[38] Por las mismas razones apuntadas y, aunque no es esta la sede para su estudio, desde la perspectiva de los atentados contra la intimidad también abogaríamos por una más adecuada redacción del artículo 198.2, tomando en consideración las importantes aportaciones de nuestra doctrina en este ámbito. Vid. por todos, MORALES PRATS, *Problemática jurídico-penal...*, cit., pp., 307 y ss.; BOIX REIG, J., *Protección jurídico-penal de la intimidad e informática*, "Poder Judicial", nº especial IX, CGPJ, Madrid, 1989, pp. 17-37.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

laboral entre sujetos activo y pasivo —como se infiere del actual artículo 499 C.P.—, bastando la obligación legal o contractual de guardar secreto, lo cual reducía notablemente el círculo de eventuales sujetos activos. En el tema que nos ocupa, esta innovación abre la posibilidad de reprimir algunos hechos hoy atípicos desde la perspectiva del artículo 499. Pensemos, a título de ejemplo, en un encargado de mantenimiento de los equipos informáticos, empleado en una empresa suministradora de *hardware*. Enviado por su empresa a realizar ciertos trabajos en los equipos de una importante compañía, descubre información reservada de la misma y la revela a otra empresa de la competencia. Igualmente, podrían ser sujetos activos del nuevo tipo propuesto, directivos y consejeros (ej: un miembro del Consejo representante del capital de una sociedad anónima), que difícilmente realizarían el tipo actual del artículo 499, por ausencia de la relación de dependencia[39].

Como en el artículo 284, también se acude en el artículo 285 a la construcción de los delitos de peligro. Basta, para la consumación, que se revele el secreto (cualquiera que desea la forma, lícita o subrepticia, de obtención del mismo)[40], poniéndose en peligro la capacidad competitiva de la empresa en el mercado, aun cuando la información revelada no hubiere sido descifrada o comprendida por aquél a quien se le comunica, y con independencia de que se haya empleado o no para producir un perjuicio económicamente valuable a la víctima[41].

En cuanto al tiempo que debe de guardar secreto, cuestión polémica en nuestros días, el Proyecto nada establece, a diferencia de la PANCP, que, en el artículo 277.3, zanjaba el viejo debate en los siguientes términos: "Si la utilización, descubrimiento o revelación se produjere después de estinguida la relación con la empresa, sólo se castigará si constituyere delito de competencia desleal"[42]. (También desaparece del Proyecto de 1992 el delito de competencia desleal que incorporaban la PANCP, y ya antes, el Proyecto de 1980).

A la vista de la pena establecida, se considera menos desvalioso el comportamiento cuando el secreto es utilizado en provecho propio. Sin embargo, también constituye una novedad en nuestro Derecho positivo su inclusión típica, pues, en el momento actual, no es punible dicha conducta[43]. En este orden de cosas, supuestos similares al que nos sirvió de introducción (ciertos empleados de una empresa informática abandonan la misma llevándose carteras de clientes, programas e información reservada de la empresa, montando su propia empresa para hacer la competencia a la anterior), parece que serían atípicos desde la perspectiva del artículo 499 C.P., pero quedarían subsumidos en el párrafo segundo del artículo 285 del Proyecto, al margen de otros delitos de daños o sabotaje informático que hubieran podido realizar.

---

[39] Vid. BAJO FERNANDEZ, *Manual de Derecho Penal*. P.E., V. II, 2ª ed., cit., p. 380.

[40] En la fórmula acogida por la PANCP se precisaba un conocimiento inicial lícito del secreto. Además, el artículo 277 prescribía expresamente que la conducta pusiera en peligro la capacidad competitiva de la empresa, frente a la regulación del Proyecto de 1992.

[41] BAJO FERNANDEZ, ult. cit., p. 382.

[42] *Ibídem.*

[43] GOMEZ SEGADE, Ult., cit., pp. 374-375.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

3. DESTRUCCION, MODIFICACION O INUTILIZACION DE ARCHIVOS Y FICHEROS INFORMATIZADOS CON VALOR ECONOMICO DE EMPRESA (SABOTAJE INFORMATICO)

En sentido análogo a la advertencia con que iniciábamos el apartado relativo al espionaje informático, debemos reflejar aquí nuestra discrepancia con los plantea momentos que abordan la temática del sabotaje informático como un todo homogéneo, sin adjetivar, y, necesariamente circunscrito a los atentados contra el patrimonio. Para nosotros, la rúbrica "sabotaje informático" debiera hacer referencia, exclusivamente, a una determinada dinámica comisiva (alteración, supresión o adicción de datos informatizados o programas en un determinado sistema para la producción de un perjuicio —no necesariamente patrimonial—, ya se actúe directamente sobre el *software*, ya sobre el *hardware*). Sin embargo, este rasgo aporta bastante poco sobre la clase de ilicitud realizada, sobre los bienes jurídicos afectados en cada caso o sobre los cauces posibles para su represión. Así, por ejemplo, y aunque la dinámica comisiva pueda ser idéntica, tienen poco en común las conductas siguientes: 1º Con el fin de perjudicar a su compañero "B" y éste vea obligado a demorar algún tiempo más la lectura de su Tesis Doctoral, "A" copia en el disco duro del ordenador de "B" un programa infectado con un virus, que destruye todos los datos almacenados en el mismo, incluida la Tesis doctoral de "B". prácticamente terminada. 2º Para provocar un caos en una empresa de la competencia, "A" interfiere en el sistema informático de aquella, borrando los archivos y ficheros informatizados relativos a su cartera de clientes y su estrategia de mercado; 3º "A", funcionario del Cuerpo Nacional de Policía, a cargo de los archivos informatizados secretos, procede a borrar una parte importante de los mismos con el fin de que desaparezcan todas las diligencias relativas al delito cometido por un pariente suyo. 4º Con la ayuda de su ordenador personal, un modem y un teléfono, "A" penetra en los sistemas informáticos de regulación de tráfico en una gran ciudad y altera el programa que se ocupa de la ordenación de los semáforos. 5º "A", empleado del INEM, desde la terminal de ordenador de su despacho, borra todos los datos informatizados relativos a las altas y bajas en dicho organismo; 6º "A" realiza la misma operación con todos los datos del sistema informatizado de cotizaciones bursátiles. Obsérvese que, no obstante haber elegido una idéntica dinámica comisiva, Esa diversidad de los bienes jurídicos eventualmente afectados impide —debe impedir— un tratamiento unitario de los casos que nos han servido de ejemplo. Es por ello, que en esta sede, sólo nos ocuparemos del sabotaje informático que afecte a programas, archivos y ficheros económicamente valuables para la actividad empresarial, es decir, los que afecten a la capacidad competitiva de la empresa[44].

La gama de procedimientos imaginables para la destrucción o inutilización del *software* resulta amplísima, estimándose que aquellos más eficaces y difíciles de detectar son, precisamente, los que se sirven de la propia tecnología del ordenador (borrado total o parcial o modificación de datos o programas, encriptación o codificación de los programas

[44] La mayoría de los autores sólo contemplan esta modalidad cuando analizan el "sabotaje informático", sin dar relevancia a otras expresiones del sabotaje contra bienes jurídicos distintos al mencionado. Vid. en este sentido ROMEO CASABONA, *Poder informático...*, cit., pp. 175 y ss.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

para imposibilitar el acceso o utilización de los mismos, introducción de "virus informáticos" o datos erróneos, etc.)[45].

Por lo que respecta a los autores, aunque es posible la realización de estos comportamientos por terceros extraños a la empresa o compañía afectadas, los estudios realizados revelan que, en la mayoría de los supuestos, quienes actúan ilícitamente son los propios empleados (*insiders*), en situaciones de conflictos laborales, —como el ejemplo citado mas arriba—[46], o como venganza personal de algún trabajador, etc. Por último, debe mencionarse en relación con la introducción de "virus informáticos" en los sistemas de procesamiento automático de datos, que no es infrecuente el que se presenten como autores los titulares mismos de los programas (el mismo titular del programa que, salvo pacto en contrario, no pierde su titularidad en caso de cesión a un tercero, prepara la alteración o destrucción del programa, o incluso de todo el disco duro para el caso de que el cesionario realice una copia ilícita o no cumpla lo acordado para el mantenimiento[47].

3.1. Cauces para el sabotaje informático empresarial en el Derecho vigente

Como ya se ha justificado anteriormente, aquí sólo hacemos referencia a las conductas de sabotaje informático que se realizan con ánimo de producir un perjuicio empresarial valuable económicamente, y que provocan, precisamente, ese resultado (con frecuencia se afecta de modo muy relevante a la capacidad competitiva de la empresa, a su posición en el mercado, a sus expectativas y estrategias de futuro, desencadenando gravísimos perjuicios económicos que van más allá de lo estrictamente patrimonial, y muy difíciles de cuantificar). Esto delimita de forma notable el marco legal de referencia para la eventual represión de tales hechos, marco legal conformado en nuestro Derecho, esencialmente, por la normativa penal en materia de daños (a falta de cualquier regulación específica para el sabotaje informático en España, cuando ya en muchos países se ha producido una reacción legislativa para aprehender las peculiaridades de estas conductas ilícitas)[48]. Es decir, nuestro punto de referencia serán los artículos 547 y siguientes del C.P.

Si la destrucción o inutilización del *software* se produce mediante la actuación directa sobre las instalaciones, edificios o equipos informáticos (*hardware*), o sobre las instalaciones o edificios donde se hallaren aquellos, no vemos obstáculo para aplicar, o bien los artículos 549 a 553 (si el medio comisivo es el incendio), o el artículo 563 (que opera como residual y tipo básico), o bien el artículo 554 (donde se tipifica el delito de estragos). Sobre la aplicación de los primeros, apunta CORCOY BIDASOLO[49] el problema que suscita la evaluación económica del perjuicio. Pues, no se olvide que el legislados establece la pena en atención al perjuicio irrogado, y dicho perjuicio, según la inter-

---

[45] CORCOY BIDASOLO, M., *Sabotaje informático, Textos de ponencias y Comunicaciones. Congreso sobre Derecho informático,* Facultad de Derecho de Zaragoza, Zaragoza, junio 1989, pp. 543 y ss., donde recoge un extenso listado de modalidades comisivas y técnicas de sabotaje informático. También, CAMACHO LOSA, L., *El delito informático*, Madrid, 1987, pp. 33 y ss.

[46] Nota 3.

[47] CORCOY BIDASOLO, Ult., cit., p. 560.

[48] Los cauces para reprimir el sabotaje informático en los distintos ordenamientos jurídicos en, SIEBER, U., *The International Emergence...*, cit., pp. 24 y ss. y 73 y ss., sobre las actuaciones internacionales orientadas a la armonización legislativa.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

pretación más extendida, hace referencia al deterioro en el valor, intrínseco o en su uso, del objeto mismo sobre el que recae la conducta prohibida, pero no a las consecuencias económicas que pudieran derivarse de ese resultado —innecesarias para el delito de daños, aunque puedan dar lugar a agravación—[50]. A nuestro modo de ver, el tema no es en modo alguno irrelevante cuando se traslada a los casos de sabotaje informático, donde el valor del soporte lógico y de los programas o ficheros destruidos o inutilizados puede ser relativamente pequeño, pero extraordinarios los perjuicios económicos derivados de esa pérdida. Se aprecia, pues, un desajuste, una falta de correlación, entre, por un lado, la concreta conducta realizada (cuya puesta en escena puede ser mínima, con actuaciones a veces tan simples como el oprimir en consola la tecla de borrado), por otra parte, los perjuicios económicos irrogados (cuantificables o imposibles de determinar), y, en fin, la pena que correspondería de aplicar las figuras anteriores (penas graduadas atendiendo al valor del soporte dañado).

El artículo 554 supera el obstáculo anterior, y es por ello que se estime por algunos autores[51] como una opción más acertada: primero, porque los estragos son interpretados como "daños de extraordinaria gravedad e importancia" y, segundo, porque no hacen pender el castigo del valor del perjuicio causado.

Cuando la conducta lesiva se proyecta directamente sobre el *software* (modificación, destrucción o inutilización, por medio de manipulación informática, de programas, archivos, ficheros o datos informatizados), parecen mayores las dificultades para la aplicación de los delitos de daño tradicionales. Como en los delitos de apoderamiento, el principal argumento esgrimido hace referencia a la determinación del objeto material: para la doctrina mayoritaria, el objeto material en los delitos de daños ha de ser una cosa ajena, mueble o inmueble, económicamente valorable y susceptible de deterioro, inutilización o destrucción[52], excluyéndose las cosas inmateriales. No obstante, pese a esta lectura clásica de los delitos de daños, compartimos la postura que en nuestros días defienden, entre otros, GONZALEZ RUS, RUIZ VADILLO, CORCOY BIDASOLO o ROMEO CASABONA[53]. Del examen de las figuras de daños se desprende que la materialidad de la cosa mueble o inmueble sobre la que recae la acción típica no es un rasgo exigido expresamente por la ley, como tampoco se exige que esa pretendida materialidad se traduzca en "aprehensividad" (en el sentido de los delitos de apoderamiento material). lo verdaderamente relevante en estas figuras es que se deteriore o dañe algo —susceptible, lógicamente, de ser deteriorado—, valorable económicamente y que pueda ser objeto de del derecho de

---

[49] CORCOY BIDASOLO, *Sabotaje informático*, cit., p. 558.

[50] BAJO FERNANDEZ, *Manual de Derecho Penal*, P.E., vol. II, 2ª ed., cit., p. 508.

[51] CORCOY BIDASOLO, ult. cit., p. 558. Vid. también, ROMEO CASABONA, *Delitos informáticos en conexión con sistemas informáticos y de telecomunicación*, cit., p. 516.

[52] BAJO FERNANDEZ, ult. cit., p. 508.

[53] CORCOY BIDASOLO, *Sabotaje informático*, ult. cit.; GONZALEZ RUS, *Tratamiento penal de los ilícitos patrimoniales...*, cit., p. 47; ROMEO CASABONA, *Delitos patrimoniales en conexión...*, cit., pp. 516-517; RUIZ VADILLO, E., *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica*, "Poder judicial", nº especial IX, CGPJ, Madrid, 1989, p. 60. (llama nuestra atención que algunos de estos autores no se muestren, sin embargo, tan partidarios de una "interpretación evolutiva" de los tipos cuando se trata de la lectura de otras figuras delictivas, como la estafa, según se indicará más adelante.).

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

propiedad. Esto permite incluir a los elementos lógicos de los sistemas informáticos entre los eventuales objetos materiales de los delitos de daños. "La alteración se produce aun cuando, sin afectar a la sustancia, se lesiona el valor de uso que la cosa tiene para el propietario. Sin olvidar que en estos casos la <sustancia> es la propia información o los datos contenidos en el fichero que se destruye, dada su autonomía respecto a los elementos físicos"[54].

Admitida la posibilidad de aplicar los delitos de daños para los casos de destrucción o inutilización de datos o programas de valor económico para la empresa, cabe mencionar, en orden de aprehender más ajustadamente el desvalor de muchos de los supuestos de sabotaje informático, los tipos agravados del artículo 558.5º y 7º C.P. En el número 5º la agravación se basa en las características del objeto sobre el que recae la conducta: "En un archivo, registro, museo, biblioteca, gabinete científico, institución análoga..." Las referencias a los archivos, registros... e "institución análoga" pudieran permitir lo aplicación de dicha agravante al sabotaje informático en ciertos casos. La agravación del número 7º, por su parte, se fundamente en el mayor desvalor del resultado: "Arruinando al perjudicado". La aptitud inicial de este precepto para castigar el sabotaje informático, normalmente caracterizado por provocar gravísimos perjuicios a la empresa, encuentra, no obstante, en el requisito de la "ruina" de la víctima, un serio obstáculo para su eventual aplicación. Plantea una situación extrema, que será necesario probar (el cierre de la empresa o la imposibilidad de continuar realizando ciertas actividades, o la paralización del proceso productivo, etc.) que no será la más habitual[55].

Con todo, no llega a convencer plenamente la solución indicada de resolver la problemática del sabotaje informático exclusivamente mediante la reinterpretación de los delitos de daños, acaso por la desconfianza que genera siempre una lectura de los tipos penales distinta a la tradicionalmente admitida, acaso porque los países cuyos ordenamientos punitivos nos sirven con frecuencia de punto de referencia, han rechazado la aplicabilidad de las tipicidades clásicas de daños y de sabotaje al "sabotaje informático", regulando, pues, la materia *ex novo*. Y si a esto añadimos la orientación que en la materia viene marcando la comunidad internacional (que, desde las distintas comisiones de Naciones Unidas, Consejo de Europa y Comunidades Europeas, recomienda a los Estados la específica regulación del sabotaje informático)[56], se entenderá que algunos de nuestros penalistas demanden también aquí la intervención del legislador, a fin de otorgar una mayor y mejor cobertura al sabotaje informático[57], "incluso sólo fuera para lograr unas penas más adecuadas al desvalor de estos hechos".

A nuestro modo de ver, lo insatisfactorio del tratamiento penal que se puede dispensar hoy en España al sabotaje informático, encuentra muy probablemente su funda-

---

[54] GONZALEZ RUS, *Tratamiento penal de los ilícitos patrimoniales...*, cit., p. 47; también CORCOY BIDASOLO, *Sabotaje informático*, cit., pp. 559 y ss.

[55] CORCOY BIDASOLO, M. *Protección penal del sabotaje informático. Especial consideración de los delitos de daños*, "Delincuencia Informática", (Comp. MIR PUIG), PPU, Barcelona, 1992, p. 175.

[56] Vid., a título de ejemplo, en COUNCIL OF EUROPE, *Computer-relatea Crime*, Recommendation No. R(89)9, Strasbourg, 1990, pp. 43-49, con una propuesta prácticamente idéntica a la solución legal en Alemania para los casos de destrucción de datos y sabotaje informático.

[57] ROMEO CASABONA, *Poder Informático...*, cit., p. 178.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

la realidad criminal que hoy tiene que afrontar. (Más que la inclusión de nuevos tipos penales que expresamente se ocupen de estos hechos, en la línea del Derecho austríaco o del Derecho alemán, acaso sería suficiente con formulaciones típicas que "no excluyeran" estas nuevas modalidades delictivas y su especialidad). Coincidimos, pues, con CORCOY BIDASOLO[58] en que la aprehensión de esta nueva realidad criminal pasa, en primer término, por una mejor regulación de los delitos de daños e incendios, y sólo en muy pocos supuestos estaría justificada la adición de nuevos tipos (v.gr. para los casos de destrucción de datos en el momento de transmisión). Por lo demás, quizá sería un buen momento para revisar, desde la perspectiva del bien jurídico, si el dato relevante para configurar estos tipos es —debe ser— siempre y en todo caso la lesión cuantificable del patrimonio.

3.2. Referencia al Proyecto de C.P. de 1992

La preocupación, en ocasiones desbordada, por llenar las lagunas que presentan las legislaciones tradicionales frente a las diversas manifestaciones de la criminalidad informática, ha llevado, en algunas legislaciones, a fórmulas excesivas, a nuestro juicio, y difíciles de justificar. Esto se detecta muy especialmente en algunas parcelas, como la que ahora nos ocupa, el llamado "sabotaje informático". En esta línea, no es extraño encontrar legislaciones que tipifican, como delito autónomo, la destrucción de datos tratados informáticamente, sea cual fuere el contenido de los mismos, y al margen del bien jurídico eventualmente afectado por tal conducta. De esta manera puede llegarse al absurdo de castigar por el mismo tipo penal, por ejemplo, la destrucción de los datos informatizados de una agenda de direcciones y teléfonos privados que tiene un sujeto particular en su ordenador personal, la destrucción de los archivos policiales informatizados, o la destrucción de los datos informatizados de una empresa de seguros, con su cartera de clientes y la planificación de su estrategia en el mercado.

Sirva como ejemplo el ordenamiento alemán, cuyo párrafo 303 a StGB tipifica el delito de *destrucción de datos*, castigando, con pena privativa de libertad de hasta dos años, o multa, la conducta de cancelar, ocultar, inutilizar o alterar datos electrónicos, magnéticos o que estén almacenados de forma no inmediatamente perceptible o que sean transmitidos. La misma Ley con la que se incorpora el código alemán este delito[59], crea, a continuación, el delito de *sabotaje informático*, castigando a quien destruye una elaboración de datos de especial significado para una fábrica o empresa ajena o una administración pública, bien mediante la conducta anteriormente definida, bien mediante la destrucción, deterioro, inutilización, eliminación o alteración de un sistema de tratamiento de datos o de los soportes de los mismos (pfo. 303 b StGB).

Una regulación de estas características, que no constituye excepción alguna en Derecho comparado y que, además, no se aparta de las recomendaciones de armonización

---

[58] CORCOY BIDASOLO, *Protección penal...*, cit., pp. 175-176.

[59] Vid. un estudio de las innovaciones de la segunda Ley de Lucha contra la criminalidad Económica, de 15 de mayo de 1986 en, MÖHRRRENSCHLAGER, M., *Das Zweite Gesetz zur Bekämpfung der Wirrtschaftskriminalität (2. WiKG)*, "Wistra", 4, 1986, pp. 123 y ss.; ACHENBACH, H., *Das Zweite Gesetz zur Bekkämpfung der Wirtschaftskriminalitat,* "Neue Juristische Wochenschrift", 30, 1986, pp. 1835 y ss.

Una regulación de estas características, que no constituye excepción alguna en Derecho comparado y que, además, no se aparta de las recomendaciones de armonización legislativa de las distintas organizaciones internacionales preocupadas por la represión de la delincuencia informática (OCDE, Consejo de Europa, Comunidades Europeas)[60], plantea notables problemas, particularmente la primera de las figuras: el delito de destrucción de datos. El que se conforme como un delito de mera actividad, sin referencia alguna al bien jurídico eventualmente afectado, puede llevar a resultados indeseables, según se indicó. El Derecho penal, a nuestro juicio, no puede emplearse para reprimir cualquier uso no autorizado de la informática. Y, aunque se ha tratado de paliar este riesgo mediante la exigencia de una efectiva lesión del bien jurídico protegido, al absoluta falta de acuerdo en torno a este punto, mantiene latente el problema[61]. Además, tampoco se olvide que se castigan por otras vías conductas de manipulación de datos informatizados más específicas, como las dirigidas a obtener un provecho patrimonial ilícito en perjuicio de otro, o las alteraciones de datos informatizados dotados de valor probatorio como ánimo de provocar un engaño en el tráfico jurídico, o el espionaje de datos para afectar a la capacidad competitiva de una empresa, etc. Queda así, por saber, si el parágrafo 303 a la del Código alemán va a quedar como vía para castigar las conductas de destrucción de datos que no provocan perjuicio alguno o sólo crean un perjuicio irrelevante. (En otros ordenamientos, como el austríaco[62], en la descripción de la conducta típica se exige la producción de un perjuicio estimable, más en la línea del delito de sabotaje informático alemán).

Por fortuna, el prelegislador español en esta materia no se ha dejado influir por esta ola "inflacionista" del Derecho penal provocada por la irrupción de las nuevas tecnologías de la información. En este sentido, no hallamos en el texto de 1992 ningún precepto asimilable al parágrafo 303 del Código alemán. Sin embargo, el juicio que cabe hacer no es del todo positivo: La única referencia que pudiéramos calificar de "más directa" al sabotaje informático (contra los valores económicos de empresa, parcela en la que hemos focalizado nuestra atención), de halla en el párrafo segundo del artículo 284.1, cuando a continuación del delito de espionaje industrial ya analizado, se establece: "Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos". Es decir, que si la conducta de espionaje informático (empresarial) va a acompañada de daños o sabotaje informático, cabe la aplicación de las reglas concursales. Claro está, si es que resulta posible castigar esos daños o sabotaje informático. El punto de referencia para resolver esta cuestión vuelve a ser, pues, la regulación de los delitos de daños, incendios y sabotaje.

---

[60] Vid., por ejemplo, COUNCIL OF EUROPE, *Computers-related Crime,* European Committee on Crime Problems, Strasbourg, 1990, pp. 49 y ss.

[61] Sobre la polémica en torno al bien jurídico, una revisión en, CORCOY BIDASOLO, *Protección penal...*, cit., p. 164.

[62] El parágrafo 126 a del código penal Austríaco, introducido por la Ley de reforma de 1987, castiga a quien *perjudica* a otro mediante la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que carezca de disponibilidad en todo o en parte. Posteriormente, el párrafo tercero establece una modalidad agravada, en atención a la entidad del perjuicio irrogado. Un estudio del alcance de este precepto en, SCHIK, SCMÖLZER, *Computer Crimes...*, cit., pp. 151 y ss.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

Entre las innovaciones que presenta el Proyecto en esta materia[63] no está, desde luego, la tipificación expresa del sabotaje informático. Pero, más aún, de la lectura de los artículos 273 a 278 (configurados como delitos patrimoniales, bajo la rúbrica "De los daños"), y de los artículos 330 a 341 (incardinados entre los delitos contra la seguridad colectiva, bajo la rúbrica "De los incendios y otros estragos"), no vemos que se pongan fin a los problemas de interpretación que hoy plantea la aplicación de esta normativa a las conductas de sabotaje informático.

Por una parte, seguirán sin plantear problemas de las conductas de sabotaje informático en las que la destrucción del *software* se lleva a cabo mediante la actuación directa sobre el *hardware*: Nada que objetar para aplicar los tipos de daños, salvo su ineptitud para aprehender el desvalor del resultado, en el sentido en que nos manifestábamos respecto al texto vigente (vid. *supra*). Y, por idénticas razones a las ya indicadas, cabría la posibilidad de aplicar los delitos de incendios y otros estragos, si bien, a la vista de la nueva descripción típica de aquí se propone el delito de estragos (art. 337), parece que debiera quedar reservado a supuestos excepcionalmente graves de sabotaje informático (por ejemplo, cuando se provoca la destrucción de las instalaciones y equipos informáticos donde se regula todo tráfico aéreo). Es más dudoso que pudiéramos reconducir por ésta vía el sabotaje informático que provoque, por ejemplo, el cierre de una empresa privada, u otros perjuicios económicos de gran entidad. Llama la atención, por último, la posibilidad de castigar los estragos producidos por imprudencia (art. 340), posibilidad que hoy está vedada, a tenor del artículo 554 vigente, que exige "causar maliciosamente".

En cuanto a los comportamientos de sabotaje directamente proyectados sobre los elementos lógicos de los sistemas informáticos, nos remitimos a las observaciones apuntadas al examinar el Derecho vigente, porque no vemos novedad alguna que permita resolver los problemas de interpretación que hoy se suscitan (vid. *supra*). En consecuencia, la subsumisión o no de estas conductas en los delitos que prevé el Proyecto, continuará al albur de la interpretación de que sean objeto.

4. CONDUCTAS DE INTRUSISMO INFORMATICO (HACKING)

4.1. En torno a la tipificación del intruismo informático

Sorprende, que, a estas alturas, cuando ya muchas legislaciones de nuestro entorno se han decidido por la represión penal de las conductas de mero intrusismo informático (*hacking*)[64], en España no ha sido abordado seriamente el tema entre nuestra doctrina. Cuando se cita, a título de ejemplo, algún supuesto de *hacking* —siempre extraído de una realidad social distinta a la nuestra—, más bien parece invocado a modo de anécdota curiosa y hasta divertida, pero no como motivo para una reflexión seria. El tema, a nuestro juicio, merece mayor atención que la de una anécdota, aunque sólo sea por algunas de las razones que apuntamos:

---

[63] Vid. GARCIA VALDES, *El Proyecto de Nuevo Código Penal*, it., p. 64, y la Exposición de Motivos del Proyecto de C.P. de 1992.

[64] Un recorrido por el Derecho comparado y la manera de afrontarse en las distintas legislaciones el intruismo informático en, SIEBER, *The International Handbook...*, cit., pp. 86-90.

1º Los estudios criminológicos realizados en otros países demuestran que, comportamientos inicialmente de mero intrusismo informático —detectados pero no reprimidos en su momento—, terminaron convirtiéndose en otros ilícitos mucho más graves, como fraudes, espionaje informático, sabotaje, atentados contra la intimidad, etc. (Descubierta la puerta de entrada a un sistema, su punto vulnerable, el *hacker* dificilmente se resiste a agotar las posibilidades que tiene a su alcance, y comete atentados contra el patrimonio, contra la intimidad, contra la seguridad del Estado, etc.[65] Se argumenta en este sentido, que castigado el *hacking* se adelanta la barrera de protección frente a hechos más graves (en este sentido deben entenderse las palabras de DEVEZE[66] cuando califica de "delito barrera" o "delito obstáculo" la figura del acceso sin autorización a un sistema informático, dentro del Derecho francés);

2º También se dice, en la misma línea, que la intervención penal en tales supuestos evita la impunidad de otros hechos, de mayor entidad, difíciles de probar. (Constando, en ocasiones, la comisión de un fraude, por ejemplo, sin embargo, lo único que puede probarse es la entrada ilícita y subrepticia al sistema. Así, no pudiendo castigar por el fraude, por falta de pruebas, que al menos podamos castigar el intrusismo, el acceso y utilización ilícita del sistema);

3º En ordenamientos jurídicos como el estadounidense, se han invocado, así mismo, razones de "educación a la población", lo que para nosotros sería "prevención general", función de motivación de la norma penal. (Como hacen notar algunos autores[67], las primeras leyes para reprimir estas conductas han realizado una función simbólica, trasmitiendo a los jóvenes desidentes de las clases privilegiadas un mensaje claro acerca del valor de la propiedad y de la "privacy"; pues, se había llegado a una situación en que la sociedad miraba con simpatía esta clase de hechos, y faltaba toda conciencia social de ilicitud —por no mencionar el conocido "síndrome de Robin Hood"[68] de los propios *hackers*—)

4º Adicionalmente, podría plantearse si acaso estuviéramos en presencia de un nuevo interés valioso afectado por estas conductas de intrusismo (interés que denominaríamos "la seguridad de los sistemas informáticos", o "confianza en el funcionamiento de los sistemas de procesamiento de datos", en la línea de otros bienes jurídicos tradicionalmente acuñados y reconocidos, como por ejemplo, "la confianza o seguridad del tráfico mercantil", "la fe pública", etc.), susceptible de recibir una protección penal autónoma[69];

5º Por último, en los distintos foros internacionales donde esta cuestión ha sido planteada, comienza a revelarse una gran preocupación por las conductas de intrusismo informático, particularmente peligrosas y difíciles de detectar y probar cuando poseen una dimensión transfronteriza, recomendándose por ello a los Estados una armonización legis-

---

[65] Recordamos el caso alemán del llamado "Chaos Computer Club", comentado por SIEBER en *The International Handbook...*, cit., p. 19.

[66] DEVEZE, J., *Commentaire de la Loi nº 88-19 du 5 janvier 1988 relative a la fraude informatique*, "Lamy droit de l'informatique", 1988, pp. 6-7.

[67] HOLLINGER, R.C., KADUCE, L., *The process of Criminalization: The Case of Computer Crime Laws*, "Criminology," vol. 26, nº 1, 1988, pp. 111 y ss.

[68] PARKER, D.B., *Crime by computer*, Charles Scribner's Sons, N.Y., pp. 12 y ss.

[69] Vid. GUTIERREZ FRANCES, *Fraude informático...*, cit. pp. 619 y 620; en este sentido, igualmente aluden a la presencia de un nuevo bien valioso vinculado al correcto funcionamiento de los sistemas informáticos, HAFT y ACHENBACH, citados en pp. 177-180.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.

lativa en torno al tema, a fin de evitar "paraisos informáticos"[70]. (España no puede mantenerse de espaldas al proceso que se está siguiendo a nivel internacional, y quizá deba plantearse algún tipo de regulación, aún cuando se establezcan los correctivos necesarios de adaptación a nuestro sistema).

Aunque, con seguridad, se argumentará en contra de la represión autónoma de las referidas conductas invocando el principio de intervención mínima, dicho argumento sólo nos llevaría a excluir en todo caso el castigo del intrusismo en sistemas o equipos informáticos menos relevantes —por razón del contenido de la información que procesan y por las funciones que llevan a cabo—. Más, subsisten las dudas respecto a otros sistemas, especialmente significativos por almacenar y procesar "información sensible" y por las funciones que tienen asignadas —y que le son reconocidas jurídicamente— en el tráfico. No se vea, pues, contradicción entre estas reflexiones y cuanto denunciábamos en sede de "sabotaje informático", pues una cosa es la protección del correcto funcionamiento de determinados sistemas "sensibles" frente a conductas de acceso ilícito, modificación de información valiosa, etc., y otra bien distinta el castigo de cualquier actuación no autorizada sobre los datos informatizados. (La experiencia estadounidense, que tantas veces nos ilustra con llamativos sucesos, en esta materia bien podría aportarnos alguna luz. Resulta significativo que, en aquel contexto, sólo hayan sido cuestionadas por la doctrina, como "exceso de reacción penal", las normas estatutarias que a nivel local castigan el mero *hacking* indiscriminadamente, pero nadie cuestione la tipificación, a nivel federal, de las conductas de intrusismo, modificación o descubrimiento de información o utilización sin autorización de los sistemas informáticos del Gobierno, o usados en su interés. Subyace a este planteamiento, a nuestro juicio, la intuición de que "no esta en juego lo mismo" en uno y otros casos, es decir, lo que entre nosotros se resolvería en sede el bien jurídico. Resulta, pues, imprescindible delimitar aquellos supuestos donde aparece oportuno otorgar tutela penal, evitando una intervención punitiva indiscriminada)[71].

Como conclusión, para nosotros el tema merece, cuanto menos, un debate en profundidad, y el momento presente, con la perspectiva de un nuevo Código Penal, pudiera resultar especialmente idóneo para ello.

4.2. Ausencia de tipificación en el Derecho vigente y en el Proyecto de C.P. de 1992

Al margen de consideraciones de *lege ferenda*, lo cierto es que, en la actualidad, son conductas impunes tanto la entrada sin autorización a un sistema informático como el llamado "hurto de tiempo" de máquina, siempre que no puedan reconducirse por las vías ya indicadas respecto al espionaje informático o sabotaje informático (no se olvide que aquí nos circunscribimos al *hacking* que afecta a información de empresa económicamente valuable, marginando en este estudio el intrusismo en sistemas informáticos que contengan información de otra índole).

---

[70] Vid. en SIEBER, *The International Handbook...*, cit., pp. 147 y ss.

[71] Sobre este tema, GUTIERREZ FRANCES, *Fraude informático...*, cit., pp. 137 y ss., citando a NIMMER y a TUNIK.

Si no han sido previstas y tipificadas expresamente en el Proyecto las conductas de daños o sabotaje informático, con menor motivo encontraremos alguna previsión para el castigo del *hacking*, el mero acceso sin autorización a un sistema informático, desprovisto de toda intención de dañar o perjudicar de algún modo a otro. No habrá, por tanto, posibilidad de reprimir comportamientos detectados en otros países, tales como la entrada telemática en el sistema de proceso automático de datos de una empresa y utilización del mismo para enviarse mensajes entre amigos, impidiendo o dificultando el funcionamiento correcto del sistema, o la interferencia en una comunicación electrónica de datos provocando una modificación o destrucción de información, etc.

FUENTE: ARROYO ZAPATERO Luis y TIEDEMANN Klaus (Ed.): Estudios de Derecho penal económico. Ediciones de la Universidad de Castilla - La mancha (Estudios ; 18), Cuenca 1994.