INFORMATICA Y DELINCUENCIA ECONOMICA EN EL NUEVO CODIGO PENAL

MARIA LUZ GUTIERREZ FRANCES
Profesora de la Facultad de Derecho de Salamanca

INTRODUCCION

Cuando fue presentado a los medios de comunicación el Proyecto de Código Penal de 1992 (verdadero soporte del nuevo Código Penal cuyo estudio ahora nos ocupa), se destacó, como una de sus atractivas novedades, la incorporación del "delito informático". Idéntica referencia se ha vuelto a escuchar en los últimos meses, si bien ya concretada en nuestro nuevo texto punitivo, el Código Penal de 1995. Buceamos sin demora en su articulado, preguntándonos: ¿Dónde incorpora el nuevo Código efectivamente "el delito informático"? En todo caso, ¿qué "delito informático"? ¿Existe, en realidad, *un delito informático*?

En plena "era de la informática", cuando pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por el ordenador y cuando prácticamente todos los sectores de las relaciones socioeconómicas dependen de la informática, también practicamente todos los delitos pueden cometerse *sobre o mediante* el ordenador. Así, por ejemplo, se puede matar manipulando el programa del ordenador al que se halla connectado un enfermo en la UVI, a fin de que se desconecte automáticamente el respirador en determinado momento; o se puede efectuar una operación de blanqueo de capitales; o se puede realizar apología del terrorismo a través de mensajes enviados por Internet, etc. En este contexto, resulta, a nuestro juicio, técnicamente inaceptable hablar de *delito informático,* como ya hemos reflejado en otro lugar (1). Debe reconocerse, sin embargo, la existencia de una nueva realidad criminal, surgida al socaire de las altas tecnologías de la informa-

ción, que interesa parcelas bien diversas del Derecho Penal (desde delitos contra la intimidad a las falsedades documentales, desde los delitos económicos hasta otros tan distantes como los delitos contra la seguridad interior y exterior del Estado, por citar algunos ejemplos), realidad criminal frente a la cual las legislaciones tradicionales no estaban preparadas.

Para adaptarse a las exigencias de esta nueva expresión de la criminalidad, la mayoría de los ordenamientos de nuestro entorno han experimentado en los últimos años importantes reformas en sus leyes penales, siguiendo las recomendaciones emitidas desde distintas instancias y foros internacionales (2). No obstante, en España el tema no ha sido considerado de interés prioritario por nuestros legisladores, excluyéndose de todas las múltiples y sucesivas reformas de que ha sido objeto el Derecho positivo desde la entrada en vigor de la Constitución. Hemos tenido que esperar hasta el nuevo Código Penal para hallar una mayor sensibilidad en materia de criminalidad informática. De la lectura global del reciente texto se infiere:

1º Que para el legislador no existe *un delito informático*, sino una realidad criminal compleja, vinculada a las nuevas tecnologías de información, imposible de reconducir a un único tipo legal (frente a otras opciones legislativas, como la seguida por la Ley francesa de 1989) (3).

2º Que, no obstante, tres han sido las parcelas más directamente afectadas en el intento por aprehender esa realidad criminal: los atentados contra la intimidad (con referencias específicas a "lo informático" en el artículo 197 del NCP); los atentados contra intereses de contenido económico (particularmente, a través de los arts. 239 *in fine*, 248.2, 256, 264.2 y 278); y las falsedades documentales, remozadas por mor del nuevo concepto de documento que suministra el artículo 26 del NCP, comprensivo también del documento electrónico.

3º Y, por último, que la contemplación en el nuevo Código de la criminalidad informática tiene lugar, no sólo a través de las específicas referencias a "lo informático", sino, además, siempre que el legislador, aun inconscientemente, *incluye*, por no *excluir* de los distintos tipos penales, su realización por medios informáticos. (En tal sentido, no será tan relevante conocer si específicamente se regula el blanqueo de capitales por medio de manipulación informática, o el fraude fiscal por medios informáticos, o el sabotaje contra la seguridad interior del Estado mediante la introducción de una *bomba lógica* o un *virus* en los sistemas informáticos de un Ministerio, por citar algún ejemplo. Más significativo será examinar si la formulación típica de los delitos correspondientes, no excluye su posible aplicación para los casos en que el ordenador esté presente en la dinámica comisiva del hecho. Porque, si es así, el nuevo Código estará aprehendiendo diversas manifestaciones de la delincuencia informática.)

Tras estas precisiones, acotamos el objeto de nuestro presente estudio: en las próximas líneas pretendemos aproximarnos a las **innovaciones que en materia de criminalidad informática acoge el legislador bajo la rúbrica "Delitos contra el patrimonio y contra el orden socioeconómico"**. De acuerdo con las orientaciones que suministran los principales estudios sobre *computer crime* dentro y fuera de nuestras fronteras, seguiremos la siguiente sistematización:

1º Infracciones patrimoniales **por medios** informáticos:

- La *estafa informática* (artículo 248.2 NCP).
- La utilización ilícita de tarjetas *electromagnéticas* a los efectos del delito de robo con fuerza (artículo 239 *in fine* NCP en relación con art. 238).

2º Atentados contra la **información** como bien de contenido económico:

- El *espionaje informático* (arts. 278 y ss. NCP).
- El *sabotaje informático* (art. 264.2 y ss. NCP).
- El *intrusismo informático* (art. 256 NCP).

Evidentemente, habremos de excluir el examen de otras parcelas de la delincuencia informática, a pesar de su innegable interés, bien por quedar alejadas de la criminalidad económica (v.gr.: los delitos contra la intimidad), bien por no representar novedad alguna en nuestro Derecho (v.gr.: conductas de piratería de programas, subsumibles en los delitos contra la propiedad intelectual ya en el viejo CP, que no sufren modificaciones de interés en el nuevo Código).

INFRACCIONES PATRIMONIALES POR MEDIOS INFORMATICOS (4)

La comunidad jurídica internacional reconoce que, dentro de la *delincuencia informática contra intereses de contenido económico,* la parcela más destacada desde el punto de vista criminológico, la más inexplorada y la que mayores problemas plantea para su detección y prevención, es la que se conoce como *computer fraud o defraudaciones mediante ordenador.* Sin ánimo de polemizar aquí en torno a su denominación, concepto y caracterización, aceptaremos, por las razones expuestas en otro lugar (5), la fórmula "fraude informático" o "defraudaciones informáticas", pero referida a una categoría de carácter criminológico, funcional –y por ello mismo, amplia–, que compendia una pluralidad de conductas lesivas de intereses económicos diversos –más allá del patrimonio individual, *stricto sensu*–, llevadas a cabo con ánimo de obtener una ventaja económica y aprovechando, en la dinámica comisiva ideal, subrepticia, engañosa, las peculiares características de los sistemas informáticos y su funcionamiento.

La doctrina penal se ha ocupado del estudio de los fraudes informáticos (bajo esta u otra denominación) diferenciando dos grupos prioritarios de problemas: primero, las *estafas* mediante manipulaciones informáticas y, segundo, las conductas ilícitas o abusivas con tarjetas magnéticas (en particular, para la obtención de cantidades en metálico de cajeros automáticos). Sin embargo, y pese a que serán estas mismas las conductas que aquí recibirán una atención especial, advertimos que nuestro concepto de "fraude informático" es más amplio, habiendo de incluirse en el mismo defraudaciones por medios informáticos contra intereses de contenido económico macrosociales (v.gr.: fraudes fiscales mediante manipulaciones informáticas; defraudaciones al sistema de la Seguridad Social; blanqueo de capitales por medio de su ocultación, transformación o conversión aprovechando las ventajas que ofrecen las nuevas tecnologías de la información; delitos bursátiles manipulando en los mecanismos informatizados de cotizaciones bursátiles; etc.), en cuyo examen no podemos aquí detenernos.

Haciéndose eco de las demandas de buena parte del mundo jurídico, el legislador español se ha decidido a afrontar el problema de los fraudes informáticos, aprovechando la oportunidad y las ventajas que representa una reforma penal global. Al efecto, el nuevo Código destina dos disposiciones con específica referencia a "lo informático", en la sede de los delitos patrimoniales:

* A continuación del tipo básico de la estafa, establece el artículo 248.2: **"También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".**

* Dentro de la regulación del robo con fuerza en las cosas, al tiempo de definir el concepto legal de llave falsa, el artículo 239 *in fine* del nuevo CP aclara: **"A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia".**

Las preguntas que, llegados a este punto, debemos afrontar son las siguientes: 1ª ¿Era necesaria esta nueva regulación, o bastaban las figuras tradicionales para hacer frente en España a los fraudes informáticos? 2ª ¿Cuál es el verdadero alcance de las previsiones referidas?

La legislación tradicional ante los fraudes informáticos

La correcta comprensión de las nuevas previsiones legales mencionadas precisa de una referencia, siquiera breve, a las lagunas detectadas en la legislación tradicional para la represión de los fraudes informáticos. Y es que, a falta de cualquier regulación específica en la materia, la doctrina y la jurisprudencia patrias han debido adentrarse en el único marco normativo hasta ahora válido, el creado por el viejo Código, para poner a prueba los tipos patrimoniales clásicos ante las nuevas conductas defraudatorias surgidas al amparo de las altas tecnologías de la información.

Estafas mediante manipulación informática en el viejo CP

Partamos de un sencillo ejemplo: "A", desde su ordenador personal y con la ayuda del teléfono y un *modem*, logra introducirse en los sistemas informáticos de la entidad bancaria "BB", realizando, mediante manipulaciones subrepticias, anotaciones ficticias en su cuenta corriente sobre ingresos sin correspondencia con traspasos patrimoniales efectivos, obteniendo un incremento patrimonial ilícito superior a diez millones de pesetas.

Según el parecer mayoritario, conductas como la anterior (clasificadas usualmente como "manipulaciones en el *input*", aunque lo mismo podría predicarse de las "manipulaciones en el *output*" y las "manipulaciones en los programas" para obtener un provecho patrimonial ilícito) difícilmente tendrían encaje en los tipos clásicos. Los argumentos esgrimidos pueden resumirse en los siguientes términos:

1º La dinámica comisiva de este tipo de defraudaciones mediante ordenador incorpora un nuevo *objeto* (de carácter inmaterial, el dinero de giro, bancario) y unos nuevos *medios* (la actuación subrepticia consiste en la manipulación de datos informatizados, dentro de sistemas de procesamiento de datos, donde es frecuente que una máquina ocupe el lugar de una persona humana). Así pues, resulta técnicamente imposible, en la mayoría de los casos, la aplicación de las figuras clásicas de apoderamiento material, al precisar estas que la conducta recaiga sobre un objeto corporal, material, tangible y aprehensible, cualidades que no pueden predicarse del dinero bancario o de un derecho de crédito. (No se olvide que son muchos los supuestos en los que el actor nunca llega al apoderamiento de una cantidad de dinero en metálico; ejemplo: mediante las anotaciones informáticas subrepticias, el autor salda una deuda con la entidad financiera. Mas, aun en los casos en que el sujeto se hace, finalmente, con una cantidad en metálico, el recurso a los delitos de apoderamiento material generaría múltiples problemas en orden a la consumación y formas imperfectas.)

2º Ante el fracaso de los delitos de apoderamiento material, acudía nuestra doctrina a la estafa (artículo 528 VCP), figura, de partida, con mayores posibilidades, al carecer de las referidas retricciones típicas por razón del objeto material: la estafa puede recaer sobre cualesquiera de los elementos integrantes del patrimonio, incluidos servicios de contenido económico y todo tipo de bienes, ya sean muebles o inmuebles, derechos reales y de crédito. Sin embargo, las dificultades que se aprecian para la aplicación del delito de estafa a los fraudes informáticos residen, según la línea doctrinal mayoritaria, en el *modus operandi* que precisa este delito: si exceptuamos las que CORCOY y JOSHI denominan "estafas informáticas fuera del sistema" (6) ("manipulaciones de datos efectuadas antes, durante o después de la elaboración del programa, quedando los datos registrados de forma asequible directamente al conocimiento del hombre"), el resto de las defraudaciones mediante ordenador resultarían atípicas (es decir, todas las llamadas "estafas por computador fuera del sistema": supuestos en los que la manipulación de datos informatizados se lleva a cabo antes o durante la elaboración del programa, de tal suerte que, a lo largo de todo el proceso defraudatorio, no aparece ninguna persona física que reciba materialmente un engaño ni realice, como consecuencia del mismo, una disposición patrimonial lesiva) (7).

3º Se ha examinado, por último, el marco normativo de las falsedades documentales, en la medida en que la mayoría de los supuestos subsumibles en la categoría de los fraudes informáticos incorpora, en su dinámica comisiva, el falseamiento de una realidad contable mediante las manipulaciones subrepticias de datos informatizados: los datos informatizados manipulados en cualquiera de las fases del procesamiento y transmisión informática no reflejan la realidad que pretenden materializar, al menos en alguna de esas fases, luego, "se plantea la posibilidad de que dicha alteración de la verdad constituya un delito de falsificación de documentos, en cuanto atentado a la fe pública de la que han de ser soporte los documentos destinados al tráfico jurídico" (8). Ciertamente, nuestra doctrina ha manifestado menos reticencias que respecto a las figuras anteriores, en orden a la aplicabilidad de algunos de los delitos de falsedades para reprimir los fraudes informáticos, si bien el concepto y características que tradicionalmente asignaba la jurisprudencia al "documento", excluiría todas las manipulaciones informáticas del programa –que no constituye un pensamiento humano en sí mismo, sino un mero instrumento de trabajo–. Con todo, la evolución sufrida por la doctrina del Tribunal Supremo en los últimos tiempos, reconociendo el "documento electrónico", ha representado un notable avance en la materia, como veremos.

A la vista de las consideraciones anteriores, nuestra doctrina mayoritaria concluía reconociendo que **el marco del viejo texto punitivo no ofrecía una garantía real de incriminación de todas las defraudaciones patrimoniales por medios informáticos, con importantes consecuencias en términos de seguridad jurídica. La interpretación flexible de los tipos penales tradicionales para superar los obstáculos por razón del objeto material de la acción o de la modalidad comisiva, no parecía posible,** según los mismos autores, **sin vulnerar gravemente el principio de legalidad penal.**

– Menos rígida nos parece, sin embargo, la postura que han acogido nuestros Tribunales. Basta examinar algunas de las escasas resoluciones que han emitido en materia de fraudes mediante manipulación informática: Así, la Audiencia Provincial de Granada, en una sentencia de 30 de noviembre de 1988, no duda en calificar como estafa un supuesto de manipulación informática fraudulenta, no obstante la inexistencia de un engaño intersubjetivo, personal, proyectado y recibido directamente por una persona física; como tampoco rechaza la aplicación, al mismo caso, del delito de falsedad en documento mercantil (art. 303 en relación con artículos 302.1º y 4º del VCP), superando cualquier reserva sobre la condición de documento de la cinta o disco magnético acumulador o estabilizador de datos informatizados. Es clara, pues, la opción de la Audiencia por una interpretación flexible y teleológica de los tipos penales, en la línea sugerida por GARCIA-PABLOS (9). Sin embargo, tal opción no coincide absolutamente con la acogida por el Tribunal Supremo. Así, en la sentencia de 19 de abril de 1991 (R. 2813) –donde resuelve el recurso de casación presentado contra la sentencia referida de la Audiencia Provincial de Granada– el Tribunal Supremo admite un concepto material de documento, en sentido idéntico a la Audiencia de Granada, pero rechaza la calificación de estafa (no considera aquí posible una interpretación teleológica del tipo de la estafa, estimándola contraria al principio de legalidad, por los mismos argumentos defendidos en nuestra doctrina). La conducta no queda, no obstante, impune, pues, habiéndose efectuado por un empleado de la entidad bancaria en cuyos sistemas informáticos se ejecutaron las anotaciones ficticias, entiende el Tribunal que cabe aplicar el delito de apropiación indebida. [Nótese que la rigidez de que hace gala el Tribunal al interpretar el tipo de la estafa, en la línea del planteamiento más clásico, sorprendentemente, desaparece al enfrentarse al delito de falsedad documental y al delito de apropiación indebida, cuestión que ya se ha valorado en otro lugar (10). Por lo demás, ¿debemos deducir que la conducta sería impune, al menos en su dimensión patrimonial, si el autor no hubiera sido un empleado del banco

sino un tercero ajeno al sistema que se hubiera introducido en el mismo a distancia?]

Manipulaciones ilícitas en cajeros automáticos en el viejo Código Penal

La irrupción en las sociedades modernas de las tarjetas con banda magnética ha supuesto uno de los acontecimientos más llamativos y revolucionarios vinculados a las nuevas tecnologías de la información. La diversidad de funciones que hoy se asignan a tales instrumentos en las relaciones normales del tráfico (instrumento de pago, instrumento de crédito, instrumento de garantía, medio codificado de acceso restringido a un espacio cerrado, etc.), da idea del complejo elenco de posibles conductas ilícitas o abusivas relacionadas con las mismas. Ciertamente, resultaría una grave simplificación pretender englobar en una categoría homogénea comportamientos tan distintos como los que citamos a título de ejemplo: utilización de la tarjeta por parte de su titular para adquirir bienes y servicios más allá del crédito concedido por la entidad emisora; utilización de la tarjeta por su titular cuando ya ha caducado o le ha sido retirada; obtención de dinero en metálico con una tarjeta electromagnética sustraída a su titular; falsificación de banda magnética de una tarjeta para obtener determinado bien o servicio de forma ilícita (ej: servicio telefónico; servicio de fotocopiadora; entrada a un garaje o a instalaciones deportivas, etc.)...

Un relevante sector de la doctrina penal española se viene ocupando, en los últimos años, de analizar pormenorizadamente la dinámica comisiva de las conductas irregulares o ilícitas vinculadas a las tarjetas con banda magnética, buscando, para cada supuesto, el posible encaje legal, dentro del marco del Derecho Penal tradicional. Comoquiera que muchas de estas conductas tienen poco en común con esa realidad criminal que denominamos delincuencia informática, con frecuencia, toda la problemática de la utilización abusiva de las tarjetas magnéticas recibe un tratamiento "próximo" a los fraudes informáticos –aunque no claramente dentro de ellos–, en la línea de algunos ordenamientos jurídicos, como el japonés (11).

Del amplio capítulo de comportamientos a que ahora nos referimos, merece una consideración especial a los autores el bloque de conductas ilícitas concernientes a las tarjetas de crédito, acaso por la espectacular importancia práctica que han adquirido en la vida económica de nuestro país, importancia que contrasta con la ausencia de cualquier regulación propia y específica en el Derecho positivo, incluido el Derecho Penal hasta el Código de 1995. En consecuencia, la referencia normativa ha debido buscarse, por un lado, en las condiciones generales y en las cláusulas de adhesión establecidas por las entidades emisoras y, por otro, en su caso, en los tipos penales tradicionales protectores del patrimonio (12).

Ciertamente, no interesa por igual a un estudio de criminalidad informática todas las posibles conductas de utilización ilícita de tarjeta de crédito, de modo que nos ceñiremos a los supuestos que sugieren mayores problemas (precisamente porque en ellos está presente esa especificidad de la informática, nota que permite caracterizar el *computer crime*): la obtención de dinero en metálico a través de manipulaciones en un cajero automático, mediante una tarjeta sustraída a su titular. Sintetizamos su consideración penal en las coordenadas del Código antiguo:

– Frente a la concepción minoritaria (22), que valora unitariamente el acto de apoderamiento de la tarjeta de crédito y el posterior apoderamiento del dinero, una significativa línea doctrinal estima que ambos hechos merecen una valoración jurídico-penal independiente, con la aplicación, en cada caso, de las reglas concursales correspondientes. Establecida tal diferenciación, la conducta que realmente interesa examinar es la utilización o uso de la tarjeta, en la medida en que, mientras ésta no sea utilizada para su destino natural, no confiere mayor ventaja patrimonial que la de su propio e intrínseco valor.

– Haciendo un repaso por las principales soluciones que doctrina y jurisprudencia arbitraban para la calificación jurídica de las con-

ductas antes reseñadas (utilización ilícita de una tarjeta de crédito para obtener dinero en metálico de un cajero automático, por parte de un tercero no autorizado), podemos resumir en los siguientes términos: Intentada sin éxito una primera vía –reconducir estos hechos al delito de estafa–, mayoritariamente se abandona el marco legal de las defraudaciones patrimoniales por razones de tipo objetivo, decantándose por las figuras de apoderamiento material y, más en concreto, por el robo con fuerza en las cosas (arts. 500, 504.4º, 510.2º VCP). Ello supone, lógicamente, admitir: primero, que el tercero, no titular de la tarjeta empleada, cuando se apodera del dinero en un cajero automático está sustrayendo una cosa mueble ajena, con ánimo de lucro y sin la voluntad de su dueño; y, segundo, que a la tarjeta de crédito sustraída a su legítimo titular se le reconoce la naturaleza de llave falsa, integrante del concepto normativo de fuerza en las cosas (arts. 504.4º y 510.2º VCP).

– Junto a esta postura, a todas luces dominante en el panorama jurídico español –acogida también por el Fiscalía General del Estado en la Consulta de 1987 (13), y por el Tribunal Supremo de modo unívoco desde entonces–, era posible hallar soluciones distintas, bien considerando impunes tales hechos según el Código Penal antiguo (14), bien admitiendo la aplicabilidad del tipo de estafa (15).

Valoración crítica y referencia a las defraudaciones informáticas en el Código Penal de 1995

El esfuerzo por reconducir las conductas defraudatorias por medios informáticos a los tipos penales vigentes, no debe crear la falsa impresión de que nuestra doctrina y nuestra jurisprudencia reconocían la aptitud plena de los mismos en esta nueva parcela de la criminalidad. Más al contrario, el sentimiento de que nuestro Derecho tradicional carecía de los resortes necesarios para afrontar esta lacra de nuestro siglo, era prácticamente unánime. Forzando, pues, la letra de la ley, era posible reprimir algunos de los referidos comportamientos fraudulentos. Pero urgía una reforma penal que, en aras a la seguridad jurídica, se hiciera eco del impacto de las nuevas tecnologías de la información sobre la realidad social, reprimiendo sus manifestaciones pervertidas. Se demandaba, pues, urgentemente, una actualización del Derecho penal en la materia. En el largo proceso de reforma penal que hemos vivido en España, por fin el Código de 1995 parece decidido a satisfacer dicha demanda, especialmente mediante las dos disposiciones ya transcritas (arts. 248.2 y 239 *in fine*), cuyo alcance para combatir el fraude informático pasamos a examinar.

La estafa mediante manipulación informática en el NCP

El antecedente inmediato del artículo 248.2 NCP lo hallamos en el Proyecto de Código Penal de 1992, donde por primera vez se tipificó expresamente la llamada "estafa informática", siendo desconocida en los Proyectos precedentes. La opción legislativa conecta con el sistema más extendido en el Derecho comparado y con la propuesta doctrinal mayoritaria que, partiendo de la especial vocación del delito de estafa para combatir los fraudes informáticos y, una vez constatados los problemas derivados de la formulación típica de dicha figura, reclamaba la incorporación al Código de un nuevo tipo de estafa, la "estafa informática", a continuación del tipo básico, que cobijara todas las manifestaciones de fraudes informáticos. Así, la nueva disposición suprime cualquier referencia al engaño (en su lugar, alude a "manipulación fraudulenta o artificio semejante"), renuncia a mencionar el error y reduce el elenco de posibles "actos de disposición" del tipo básico a "la transferencia de cualquier activo patrimonial en perjuicio de tercero". En suma, elimina los obstáculos que, al menos aparentemente, impedían aplicar el delito de estafa a las defraudaciones mediante ordenador.

De una primera lectura del precepto se infiere que, a partir de ahora, podrá reprimirse en nuestro ordenamiento cualquier modalidad de manipulación informática (manipulaciones en el *input*, en el *output*, en los programas y en transmisión electrónica de datos), conoci-

da o por conocer (idea que expresa con la fórmula analógica "o artificio semejante"), que provoque una transferencia patrimonial ilícita, siempre que sea dolosa y se actúe con ánimo de lucro. Por lo demás, la inexistencia de limitaciones respecto al sujeto activo permitirá castigar este tipo de conductas cuando se realicen a distancia por terceros ajenos al sistema informático.

Sin embargo, debemos expresar aquí nuestras reservas en torno al verdadero alcance de este nuevo tipo. Pues, para nosotros, como intentaremos explicar, su virtualidad respecto a los fraudes informáticos es bastante limitada. 1º Porque, en el mejor de los casos, sólo servirá para combatir una parcela de los fraudes informáticos: aquellos que supongan un ataque al patrimonio, como bien jurídico de carácter individual microsocial. Al contemplarse como una modalidad de estafa, sin otra peculiaridad que lo concerniente a su dinámica comisiva, se verá afectada, lógicamente, de las mismas limitaciones por razón del objeto jurídico que este delito. Y no se olvide que la estafa se configura como un delito contra el patrimonio individual, que ya ha revelado (16) su inidoneidad frente a otros ataques a bienes jurídicos colectivos de naturaleza socioeconómica, tales como el sistema de cotizaciones bursátiles, la Hacienda Pública en su vertiente de ingresos o en su vertiente de gasto público, el sistema de la Seguridad Social, etc. Mas, aun dentro de los ataques al patrimonio, queda sin resolver si será en todo caso de aplicación el nuevo artículo 248.2, o cederá frente a figuras como la apropiación indebida, en atención a la vinculación del autor con los fondos. 2º Limitada porque, a nuestro entender, declara que son estafas los fraudes informáticos que ya hubieran tenido cabida en el artículo 528 del Código anterior (los fraudes informáticos *contra el patrimonio*). Por tanto, consideramos que su papel se circunscribe a servir de cauce para resolver, por la vía de la interpretación auténtica (para evitar interpretaciones contradictorias, en detrimento del principio de seguridad jurídica), los problemas de interpretación que venía planteando el tipo de estafa en relación con las "estafas mediante manipulción informática".

Ahondaremos en esta reflexión –que sabemos polémica-: Para nosotros, insistimos, la nueva figura se limita a declarar que son estafas comportamientos que ya merecían tal calificación. Urge, pues, una revisión a la lectura tradicional del tipo de estafa. Como ya hemos justificado en anteriores trabajos (17), entendemos que la regulación de la estafa en España, particularmente a partir de la reforma por L.O. 8/1983 de 25 de junio, posee una mayor virtualidad ante el *computer fraud* que la que se le viene reconociendo. Abordamos la cuestión por un doble frente: uno primero, donde nadie dudaría en afirmar la estafa (aquellos supuestos en los que el resultado de la manipulación informática es percibido y aprehendido por una persona física, que conoce la significación de los datos alterados, y que ordena una disposición patrimonial lesiva a consecuencia de la falsa representación mental de la realidad a que se le induce); y, un segundo frente, más problemático a los efectos de apreciar la estafa, cuando los fraudes se efectúan sobre sistemas informáticos total o parcialmente automatizados, que operan con autonomía de la puntual intervención de personas físicas y que, incluso, están programados para efectuar disposiciones patrimoniales. El primer bloque de supuestos no ofrece dificultades en la afirmación de la estafa, cualquiera que sea la interpretación del tipo básico (se aprecian todos los elementos objetivos que exige la construcción clásica de este delito, incluidos los más problemáticos, la constancia de un estado psicológico de error en la víctima del engaño y el que la víctima, una persona física, realice materialmente la disposición patrimonial lesiva). La discusión afecta a la segunda categoría, que es, sin duda, la más relevante desde el punto de vista práctico, por comprender todos los supuestos de fraudes informáticos relativos a los sistemas electrónicos de transferencia de fondos (sistemas que ya operan en todas las grandes empresas y entidades, y a cuya implantación y generalización tiende el desarrollo tecnológico más moderno). Para que la estafa pueda tener alguna virtualidad en este

último terreno consideramos necesarios, por lo menos, dos presupuestos: uno, vinculado a los propios ordenadores y a su función instrumental, y otro, referente a la conformación del propio tipo de estafa.

1º Por obvio que parezca, lo primero que se precisa es el correcto entendimiento del papel que hoy juegan los ordenadores y, especialmente, en las relaciones del tráfico. Pues, aún encontramos autores –y sentencias– que atribuyen a estas máquinas cualidades, funciones y responsabilidades propias de las personas. Sean cuales fueren su complejidad, grado de sofisticación y funciones asignadas, los ordenadores son meros instrumentos, aparatos creados por el hombre y a su servicio, a los cuales se prepara, programa y dispone para que ejecuten, en concreto, órdenes determinadas. Respecto a un comportamiento fraudulento, el ordenador sólo podrá ser "objeto" o "instrumento", pero nunca "víctima" o "sujeto de la acción". Debe, pues, desterrarse la inexacta apreciación de la realidad de las cosas que subyace tras expresiones como "engaño a una máquina", "máquina engañada", "ordenador engañado que realiza por error el acto de disposición", y similares. Porque, ni se engaña a la máquina–ordenador (a lo sumo, se engaña a alguien utilizando como instrumento la máquina), ni el ordenador realiza por error acto alguno de disposición (en todo caso, se limita a "ejecutar", en concreto, el traspaso patrimonial ordenado y dispuesto por quien ha efectuado la programación, único que tiene el dominio de la disposición patrimonial). Nótese que lo único que en realidad estamos reclamando es que se admita, dentro de nuestra disciplina, lo que ya reconoce todo el resto del ordenamiento jurídico: las nuevas formas de concertar y ejecutar negocios jurídicos que, por razones de celeridad, se han incorporado a la vida moderna.

2º Se precisa, además, una determinada interpretación del tipo de estafa -distinta a la que se viene arrastrando de un modelo superado de relaciones económicas– que sistetizamos en los puntos siguientes:

– Respecto al engaño típico, es imprescindible aceptar que el falseamiento de la realidad que el engaño implica, no comporta necesariamente una relación "directa y personal" entre dos seres humanos, emisor y receptor. Hay que huir, pues, de tal exigencia de inmediatez, deducida por vía de interpretación, y sólo comprensible en otro contexto histórico, en el cual dicha nota caracterizaba las normales relaciones del tráfico jurídico. Por lo demás, en tanto se siga negando –en Derecho penal, que no en otras ramas del ordenamiento– la posibilidad de engañar a una persona jurídica, o a cualquier persona, física o jurídica, cuando actúa en el tráfico con el auxilio de las altas tecnologías de la información (postura que no compartimos), la figura de la estafa quedará vedada a la mayoría de las defraudaciones informáticas, particularmente a las que afectan a sistemas automatizados de toma de decisiones.

– Respecto al error, ya hemos manifestado nuestra preferencia por la línea que le niega la condición de elemento autónomo del tipo de estafa, circunscribiendo su función a la delimitación restrictiva del engaño típico. Siguiendo una interpretación de esta índole quedarían suprimidos, en efecto, algunos de los obstáculos que aquí se invocan para calificar como estafa las defraudaciones con ordenador. Sin embargo, de continuar reconociéndole al error aquella condición de elemento autónomo, como hace la doctrina mayoritaria, la aplicabilidad de la estafa al grueso más relevante de fraudes informáticos pasa por el abandono de la "concepción psicológica del error" (estado psicológico de la "persona humana" consistente en una falsa representación mental de la realidad). Desde luego, si se exige para la estafa la constancia de un estado psíquico de error en la víctima del engaño, detonante de la disposición patrimonial, nada tiene que hacer este delito en el terreno de los fraudes mediante computadoras, a excepción del reducido círculo de supuestos que antes calificábamos como "no problemáticos".

– En lo que respecta al acto de disposición, también sería precisa una interpretación –consecuencia natural de un entendimiento distinto del engaño y del error–, asumiendo,

con el resto del ordenamiento jurídico, que se pueden realizar disposiciones patrimoniales con el auxilio de una máquina. Como ya hemos defendido, la escisión temporal entre el momento volitivo y la concreta ejecución de la disposición patrimonial no debe llevar a confusión, pues el dominio de la disposición no corresponde al ordenador –que sólo materializa órdenes que se le han introducido–, sino al que prepara los equipos informáticos y los programa para operar, o al que encarga hacerlo, ya sea persona física o jurídica. Mas, si la disposición patrimonial requerida por el tipo de estafa se considera en el sentido tradicional, restringida a los traspasos de bienes materialmente ejecutados por un hombre, a consecuencia del estado psicológico de error que se le ha provocado por engaño, poco le resta por hacer a la estafa respecto al fraude informático.

Una propuesta interpretativa de este orden que, por no ajustarse al planteamiento de la estafa clásico, pudiera parecer que conmociona las estructuras más íntimas y esenciales de este delito, no goza, en nuestros días, de un apoyo doctrinal y jurisprudencial suficiente, al menos como planteamiento teórico inicial. Sin embargo, curiosamente, algunos autores que, de partida, se mantienen fieles a la construcción clásica, acaban renunciando a la misma en la práctica, al tiempo de resolver, en concreto, la calificación de ciertos supuestos de hecho problemáticos: así, por ejemplo, quienes afirman la estafa en los casos de manipulación en aparatos automáticos para obtener ilícitamente un bien o servicio (18); o en las manipulaciones ilícitas de cajeros automáticos (19). Es decir, se observa un reconocimiento implícito de la lectura del tipo básico que sugerimos, pese a la adhesión previa inicial a la interpretación mayoritaria.

En consecuencia, las objeciones de mayor consistencia que cabría oponer al nuevo entendimiento del tipo de estafa, a nuestro modo de ver, no pueden estar basadas en el principio de legalidad penal, como se desprende de un examen detenido de cada uno de sus elementos. Pues, tan acordes –o contrarios– al principio de legalidad como estas soluciones indicadas resultan otros criterios interpretativos de unánime aceptación (v.gr.: la equiparación de la fórmula legal "engaño bastante para producir error en otro" y la lectura doctrinal "bastante engaño que produce error en otro"; o la subsumción de la disposición patrimonial por mera tolerancia, incluso inconsciente, dentro de la expresión "induciéndole a realizar un acto de disposición". ¿Cómo defender esto y rechazar, a continuación, por ejemplo, la disposición patrimonial ejecutada con el auxilio de un sistema informático? La diferencia de fondo estriba en el mayor o menor arraigo e implantación de las diversas interpretaciones; **luego, los problemas, antes de la incorporación del artículo 248.2 NCP, eran más bien de seguridad jurídica, al quedar finalmente al arbitrio del tribunal sentenciador la calificación como estafa de las defraudaciones informáticas. El alcance de la nueva disposición será, pues, limitado. Por razón del bien jurídico y porque, a tenor del mismo, "se consideran estafas" conductas que *eran* estafas.** Por lo demás, quede patente nuestro recelo hacia el intento que representa el precepto examinado de pretender describir ¡nuevamente! las distintas modalidades de conducta posibles –que, en realidad, son distintas formas de engaño–; pues bien pudiera interpretarse como un paso atrás, una vuelta al sistema casuístico anterior a la reforma de 1983, cuando el legislador se afanaba, en vano, en señalar las formas inimaginables de engañar (¿intentar, otra vez, el "poner puertas al campo"?).

En relación con la asimilación de las tarjetas magnéticas al concepto legal de llave falsa

La solución del artículo 239 *in fine* del nuevo CP, por su parte, también permite una doble valoración: Primero, positiva, en la medida en que se unifican criterios de interpretación, poniéndose fin al desconcierto creado por soluciones jurisprudenciales contradictorias, lo que supone un paso significativo en términos de seguridad jurídica. (Con todo, es preciso reconocer que el mérito de la unifi-

cación de criterios corresponde a la Fiscalía General del Estado, como ya se indicó.) Sin embargo, es posible, a continuación, cuestionar dicha opción, al imponer una solución unívoca para supuestos de naturaleza bien distinta, dejando subsistentes relevantes lagunas –o, cuanto menos, nuevas dudas–. En efecto, al catalogar como llave falsa todo tipo de tarjeta, magnética o perforada, así como los mandos o instrumentos de apertura a distancia, incurre el Código en una simplificación, desconociendo que existen múltiples variedades de tarjetas, que, ni por su naturaleza ni por sus funciones, se pueden asimilar. Pensemos, a título de ejemplo, en los siguientes casos: 1º "A" sustrae, de la recepción de un hotel, la tarjeta con banda magnética de apertura de la habitación 502 mientras su ocupante está ausente. Con la ayuda de la tarjeta accede a la habitación 502 y se apodera del dinero y las joyas que allí guardaba el cliente. 2º "A" se apodera de la tarjeta perforada destinada a la apertura de la caja fuerte de "B", abre la misma y se lleva, sin autorización, todo el dinero de su interior, propiedad de "B". 3º "A" encuentra el billetero de "B", con su tarjeta de crédito con banda magnética y su número de identificación personal. En un cajero automático hace uso de ella y obtiene ilícitamente una suma de dinero en metálico. 4º "A" obtiene, a través de un cajero automático y por un procedimiento similar al anterior, la misma cantidad de dinero, pero, en este caso, con la libreta de ahorros de "B" provista de banda electromagnética.

Pese a la aparente proximidad de los supuestos anteriores, existen notables diferencias entre ellos. Desde un punto de vista técnico, la conducta en los dos primeros supuestos obedece a la dinámica comisiva de los delitos de apoderamiento material. La tarjeta, en uno y otro caso, cumple materialmente la función de una llave, y es empleada por el sujeto activo para superar el obstáculo con que el titular protege sus bienes. Superada dicha barrera de protección, "A" se apodera de las cosas muebles ajenas "contra" la voluntad de su dueño. En cambio, en los supuestos tercero y cuarto, la conducta de "A" responde a la dinámica de las defraudaciones: al presentarse ante el cajero con la tarjeta –o la libreta dotada de banda magnética– y teclear el código de identificación personal, se presenta ante la entidad bancaria como si fuera el legítimo titular o la persona autorizada por el titular (20). Se crea, pues, a la entidad, una falsa apariencia de la realidad –aquí, a través del cajero automático, pero sucedería lo mismo si tal conducta se llevase a cabo ante el cajero, persona física, colocado tras una ventanilla del banco–. El banco, que, por ser persona jurídica tiene que operar en el tráfico mediante personas físicas y/o máquinas, se representa, falsamente, que tiene delante al titular de la tarjeta, y atiende a su petición de dinero de forma voluntaria, aunque sea un consentimiento viciado por error. Es decir, la disposición patrimonial se efectúa con, y no contra, el consentimiento del banco, consentimiento obtenido mediante el eficaz despliegue de la acción engañosa. El solo hecho de que, finalmente, el sujeto se lleve la suma de dinero ajeno, no muta en absoluto la naturaleza del comportamiento, en el que prima lo fraudulento como medio para conseguir de la víctima una disposición patrimonial voluntaria. Entendemos, en consecuencia, que la solución idéntica para todos los supuestos de esta índole, aunque aporta una buena dosis de seguridad jurídica, técnicamente no es la más adecuada.

Nos referíamos, por último, a la posible subsistencia de lagunas (o, al menos, problemas de interpretación), y el último de los ejemplos mencionados es buena prueba de ello: ¿Qué tipo penal debiera aplicarse, a la vista de la nueva regulación, a los casos en los que es una libreta de ahorros con banda magnética –por ejemplo–, y no una tarjeta, el instrumento para la comisión del delito? La libreta no puede, en rigor, considerarse una tarjeta magnética o perforada ni un mando o instrumento de apertura a distancia, luego no cabe su consideración como llave falsa. Y, ¿qué futuro espera a las conductas de obtención ilícita de bienes y servicios mediante la manipulación de aparatos automáticos? ¿Seguiremos en la incertidumbre que genera el actual "peregrinaje" por las distintas figuras contra el patrimonio, con soluciones tan dis-

pares como la impunidad, la estafa o el hurto? (21). ¿Qué solución tendrán que aplicar los tribunales ante la utilización ilícita de tarjetas con banda magnética manipulada para la obtención de un servicio (ej: tarjetas para llamar por teléfono), que no admite la calificación de robo por razón del objeto material del delito? Por lo demás, no olvidamos que la criminalidad vinculada al uso ilícito de tarjetas magnéticas en nuestros días es bastante más compleja: existe todo un submundo de verdaderas mafias, mercados negros y redes de "producción", "distribución", "falsificación" y "manipulación de bandas magnéticas" que producen pingües beneficios. En todo este entramado, la nueva disposición que se incorpora al Código de 1995 sólo podrá recaer, en el mejor de los casos, sobre el último eslabón de la cadena, manteniéndose intactos los problemas de calificación de las conductas precedentes. Y, una última duda: ¿serán tratadas, a tenor de este precepto, las manipulaciones en la tarjeta o en la banda magnética como una manipulación o duplicación ilícita de cualquier llave, puesto que a las llaves han sido asimiladas, es decir, como hecho impune? ¿o como una falsedad en documento mercantil? (No deja de resultar chocante un posible concurso medial entre un delito de falsedad documental y un delito de robo con fuerza, con dinámicas comisivas tan opuestas.)

Debemos concluir este apartado matizando el optimismo con que se ha recibido esta disposición. Mucho nos tememos que los tribunales van a hacer pocas excepciones y que, más allá de la dinámica comisiva que presida el hecho, calificarán como robo con fuerza prácticamente toda defraudación donde "aparezca" una tarjeta magnética, siendo así que **buena parte de estos supuestos encontraría su adecuado encaje en la estafa.**

ATENTADOS CONTRA LA INFORMACION COMO VALOR ECONOMICO DE EMPRESA

La informática ha incidido de forma insospechada en el viejo concepto de "la información", hasta el punto de transformar una mera acumulación de datos en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico. Uno de los sectores más afectados por este fenómeno es el de la actividad empresarial e industrial. El mundo de la empresa ha 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; así, la informatización implica, en nuestros días, contabilidades, carteras de clientes, balances, informes y proyectos empresariales, estrategias de mercado, procedimientos económicos o tecnológicos de carácter reservado, o datos de investigación y desarrollo de 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 ilícitas de diversa índole (contrapunto de las ventajas que el uso de los sistemas de proceso automático de datos comporta).

En las próximas líneas, **nuestra atención se centrará en la "información"** (almacenada, tratada y transmitida mediante los sistemas de procesamiento de datos), **como valor económico de empresa** que confiere a su titular una posición ventajosa en las relaciones del tráfico económico. Como interés social valioso digno de la tutela penal, nos acercaremos a **las vías instauradas por el nuevo Código Penal para su protección,** frente a los comportamientos ilícitos que más gravemente pueden atacarlo, conductas susceptibles de engrosar alguna de estas tres grandes categorías: 1º El **espionaje informático** industrial o comercial; 2º Las conductas de daños o **sabotaje informático;** y 3º Las conductas de **mero intrusismo**, también conocidas por el término anglosajón *"hacking"* (22).

Como tendremos ocasión de comprobar, las fronteras entre estas grandes categorías no son siempre nítidas. La dinámica comisiva propicia las situaciones concursales. Así, no será infrecuente que un comportamiento de espionaje empresarial vaya acompañado de una modificación o destrucción de datos, subsumible en la categoría de sabotaje informático; o que la intrusión subrepticia de un *"hacker"* en un sistema de procesamiento automático de datos desemboque en una modificación o supresión de datos, de extraordinarias consecuencias económicas para la víctima, lo cual nos trasladaría desde el intrusismo informático a los terrenos del sabotaje. (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 (23). 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) (24). En consecuencia, será la dimensión subjetiva de la conducta la que, con frecuencia, nos aporte el criterio delimitador en cada caso.

1. Espionaje informático industrial o comercial en el nuevo CP

Frente al planteamiento doctrinal más extendido, consideramos imprescindible la adjetivación del concepto "espionaje informático" con las referencias a lo "industrial" y "comercial" (empresarial) (25). 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, con ánimo de lucro y sin autorización, de los datos almacenados en un fichero informatizado (nosotros apuntaríamos, además, "de valor para el tráfico económico de la industria o comercio").

Señala ROMEO CASABONA (26) 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 memorización 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.

Hasta el Código Penal de 1995 no ha existido, en punto al espionaje informático empresarial, una regulación específica en nuestro Derecho punitivo, a diferencia de otras legislaciones próximas, como la alemana, austriaca, griega, italiana, etc. (27). Antes, pues, de ahondar en el nuevo marco jurídico que configuran básicamente los artículos 278, 279 y 280 NCP, sistetizaremos las principales objeciones que ha merecido la antigua regulación.

1.1. *Antecedentes: limitaciones del viejo Código Penal*

En aras a detectar la virtualidad de las figuras tradicionales en la materia que ahora nos ocupa, nuestros penalistas han recorrido

exhaustivamente el viejo texto penal, llegando a las conclusiones que en esencia resumimos:

1º Como punto de partida, se ha rechazado 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 (28) "que los elementos lógicos (*software*, ficheros) no son, sino un conjunto de información, ideas o instrucciones que se recogen en un medio al que se accede eléctricamente. Unas veces, en 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".]

2º El recurso a las disposiciones –civiles y/o penales– protectoras de la propiedad intelectual, aunque posible, se estimó también como 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) (29), sólo cabría 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 tuviera, 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 tuviera el carácter de "secreto", requisitos que difícilmente serán aplicables a archivos informatizados sobre carteras de clientes, balances, recopilaciones de direcciones, etc., cuyo valor, por lo general, radica en que su conocimiento es reservado.

3º Como vía alternativa, se han puesto a prueba los delitos de descubrimiento y revelación de secretos (arts. 497 y ss. del Código antiguo, en un Capítulo conflictivo, integrado por atentados contra bienes jurídicos de naturaleza diversa). Pues bien, en un rápido repaso por estos preceptos se comprueba lo insatisfactorio de dicha opción:

– El artículo 497 VCP., destinado, según el parecer más extendido, a la protección del bien jurídico "intimidad personal", sólo mediante una interpretación forzada hubiera servido para la tutela del secreto industrial. Mas, otros obstáculos derivados de su formulación típica han sido estimados como verdaderamente limitativos de la virtualidad del precepto respecto al espionaje informático: el objeto material del delito (secreto incorporado en "papeles o cartas", que veta el referido precepto a los casos en que la información reservada interceptada no hubiera sido objeto de impresión en "papel") y la conducta típica (la conducta de "apoderamiento" se interpreta clásicamente como una exigencia de traspaso material, requisito que difícilmente hallamos en los supuestos de espionaje informático). Sus posibilidades, pues, para castigar la copia de elementos lógicos de los sistemas informáticos económicamente valuables y con ánimo de lucro eran más bien escasas.

– También el artículo 498 VCP 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 (30). Mas, el que nuestra jurisprudencia haya considerando estos preceptos como intercambiables (31), unido a la formulación típica del artículo 498 –donde resulta irrelevante el soporte al que se incorpora el secreto y que su divulgación se haga con ánimo de lucro–, abriría las posibilidades de esta figura en el ámbito del espionaje informático. En cualquier caso, su virtualidad siempre se ha visto limitada: por razón del sujeto activo ("administrador, dependiente o criado", 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 (la exigencia de "divulgación" de los secretos que excluye el mero descubrimiento, lectura de datos en pantalla o su utilización por el propio autor). El sujeto activo tendría que hallarse en situación de conocimiento lícito del secreto, pues, caso contrario, como apunta GONZALEZ RUS, hubiera resultado preferente el artículo 497 (32).

– El artículo 499 antiguo, por el contrario, a pesar de su criticable incardinación sistemática, sí parecía, *a priori*, dotado de una mayor aptitud para reprimir los supuestos de espionaje industrial informático, al erigirse en el instrumento único que arbitraba nuestro viejo Código para proteger penalmente el secreto industrial o comercial. Las posibilidades de aplicar esta figura a las conductas que nos ocupan se veía favorecida por algunos de los rasgos de su descripción típica. Así, por razón del bien jurídico, la doctrina más extendida ha entendido que persigue la protección de la capacidad competitiva de la empresa en el mercado (el bien que resulta afectado por el espionaje informático empresarial). Se castigaba el hecho de "descubrir", entendido como "revelar", el secreto. Pero, ni se exigía que el sujeto activo comprendiera el contenido de lo que revelaba, ni la consumación precisaba de la producción efectiva de un perjuicio económico estimable, cuantificable (33). No habiendo delimitado el legislador el elenco de conductas típicas, parecía 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 debiera tener acceso al secreto por un cauce lícito, de modo que cabría subsumir los supuestos de obtención subrepticia de los datos o ficheros informatizados y su posterior transmisión. Sin embargo, sus posibilidades respecto a los casos de espionaje informático resultaban muy mermadas, por el estrecho círculo de posibles sujetos activos ("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" (34). Quedaban excluidos, 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, constituía una grave laguna. Tampoco podía reprimirse la conducta del empleado que conoce por 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). En suma, se consideraba una solución insuficiente e insatisfactoria para la problemática que hoy representa, en las sociedades modernas, el espionaje industrial –informático y no informático .

– El artículo 497 bis del texto anterior, por último, también ha sido estimado como dotado de cierta aptitud para reprimir el espionaje informático, aunque solventando el escollo, nada insignificante, del bien jurídico (para la opinión mayoritaria esta figura se orientaba a la protección de la intimidad, quedando, en principio, excluida la tutela del secreto industrial). Salvando tal obstáculo, ha sido aceptada su validez, por ejemplo, ante supuestos en los que se intercepta la información reservada en la fase de transmisión electrónica de datos de una terminal a otra, o aquéllos en los que se instalan los artificios técnicos para interferir o reproducir tal información (35).

4º Respecto a ficheros o bancos de datos informatizados que posean el carácter de reservado o secreto, aún cabría el recurso a la normativa que se ocupa de la protección de la competencia. Ello nos remite, en la actualidad, a la Ley 3/1991, de 10 de enero, de Competencia Desleal (36), donde hallamos un cauce de tutela posible, de naturaleza extrapenal –y acaso más efectiva– del secreto industrial, incluido el secreto industrial incorporado a archivos o registros informatizados (arts. 13 y ss.). Evidentemente, no es esta la sede para el examen de dicha norma, pero no podemos dejar de mencionarla habida cuenta de su importancia, incluso tras la

entrada en vigor del nuevo CP, texto carente de cualquier previsión específica para reprimir la competencia desleal (a diferencia de Proyectos precedentes) (37).

5º Por lo demás, aún quedaba abierta una última posibilidad, sólo para casos de espionaje informático industrial en que la conducta hubiere recaído sobre 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): en el marco normativo del antiguo Código cabía la aplicación del artículo 534, con remisión, en último extremo, y por mor del empleo de la técnica de la ley penal en blanco, a la legislación 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 la informática concierne, la Ley de Protección Jurídica de las topografías de los Productos Semiconductores, de 3 de mayo de 1988 (38).

Como **conclusión** a este tortuoso peregrinaje, **la doctrina penal apostaba por una adecuada represión de las conductas de espionaje industrial, que no desconociera esa dimensión del mismo que denominamos "espionaje informático", y con ubicación sistemática en su sede idónea: el marco de los delitos económicos.**

1.2. *Espionaje informático en el nuevo Código Penal*

Como punto de partida, debemos valorar positivamente la opción sistemática del nuevo CP. Pues, las dudas que ha suscitado el bien jurídico protegido en los delitos comprendidos bajo la rúbrica "Del descubrimiento y revelación de secretos" en el viejo Código, 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 formalmente en el nuevo texto punitivo. Ahora se delimitan con nitidez las parcelas: 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. 197 ss. NCP) y, por otra, los atentados contra los secretos empresariales o industriales –se hallen o no informatizados– (arts. 278, 279 y 280 NCP).

Los cauces fundamentales que ahora se ofrecen 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.

1º Desde luego, a la vista del texto, continúa abierta la posibilidad de aplicar las disposiciones que protegen la propiedad intelectual. Como en el sistema anterior, es imprescindible que las conductas de espionaje informático se hallen descritas en el artículo 270 NCP y recaigan sobre un programa en el sentido de la Ley de Propiedad Intelectual, o sobre bases de datos, archivos o registros informatizados cuyo contenido sea una de las obras protegidas por la legislación indicada.

2º Tampoco vemos obstáculo para aplicar 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 273, 274 y 275 NCP. (Hacemos notar que se abandona la técnica de la ley penal en blanco, al menos formalmente, ya que continuará resultando imprescindible el recurso a las leyes de contenido extrapenal, bien por expresa remisión de los nuevos tipos, bien por la necesidad de interpretar los elementos normativos empleados en estas figuras.)

3º Sin embargo, aún hallamos en el texto de 1995 otras disposiciones más directamente vinculadas a los comportamientos de espio

naje informático empresarial o industrial, de cuyo examen pasamos a ocuparnos:

– Artículo 278.1: **"El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses".**

2. **"Se impondrá la pena de prisión de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos".**

3. **"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".**

– Artículo 279. **"La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.**

Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior".

– Artículo 280. **"El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses".**

Una primera lectura conjunta de estos preceptos, sugiere las siguientes reflexiones:

1º Su incardinación sistemática, dentro de los "Delitos contra el patrimonio y contra el orden socioeconómico", debe contemplarse como un notable avance respecto al antiguo Código. Y la remisión del artículo 278.1 a "los medios o instrumentos señalados en el apartado 1 del artículo 197", no debe interpretarse como un puente que liga *todavía* a unas y otras infracciones (las que atentan contra la intimidad y las que atentan contra el secreto industrial). Más al contrario, sólo confirma la idea de que los artificios informáticos (como los demás señalados en el art. 197) pueden servir de instrumento a ilícitos de muy diversa índole sin mutar, por ello, su naturaleza. Aunque la dinámica comisiva en ambos delitos llegue a coincidir, el dato verdaderamente relevante es el bien jurídico, y en este punto nunca podrán confundirse.

2º En clave de bien jurídico todavía y, en la línea de razonamiento que aceptamos respecto al artículo 499 anterior, entendemos que los nuevos artículos 278, 279 y 280 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. Mantenemos esta interpretación apelando a la rúbrica del Título en que se hallan incardinadas dichas figuras, que lleva a exigir un atentado de intereses económicos; ello, a pesar de que, en última instancia –y no entendemos por qué–, el legislador ha suprimido toda referencia a la naturaleza del secreto, referencia clarificadora que sí constaba en el Proyecto de 1992, y que el legislador parece haber considerado superflua. La cuestión puede tener trascendencia, por ejemplo, respecto a las conductas de intrusismo informático que persiguen, exclusivamente, descubrir la clave o vía secreta de acceso a los sistemas informáticos de la empresa. Pues, la falta de concreción sobre el contenido del "secreto" en las disposiciones que comentamos, pudiera llevar a incriminar tales hechos (solución que estimamos insostenible desde la perspectiva del bien jurídico).

3º En cuanto al objeto material del delito (delitos, en este caso), 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 (interpretación

coherente con lo indicado en sede de bien jurídico).

4º Si examinamos separadamente estas figuras para conocer sus posibilidades en la represión del espionaje informático industrial, llegamos a las siguientes conclusiones:

– En relación con el artículo 278.1, el bien jurídico tutelado y el objeto material del delito suministran una importante vía de acceso a los ilícitos informáticos que aquí se examinan. Pese a la restricción que representa la exigencia de que la información afectada tenga carácter secreto, deja claro el legislador que, a los efectos de la protección, resulta irrelevante el soporte al que el secreto –la información reservada– se encuentre incorporado. (Recordamos que este punto tampoco representaba un problema a la luz del anterior artículo 499, que incluía –por no excluir– los archivos y bancos de datos informatizados secretos.)

En cuanto al sujeto activo, se superan, con acierto, las limitaciones del artículo 499 VCP, que dejaba fuera 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 nuevo texto, sea cual fuere el sujeto activo y su vinculación con la entidad afectada. (Sólo sería de aplicación el artículo 279, 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 278.1 para su consumación–.)

Sin embargo, aun reconociendo el logro 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 la 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 sin dificultad las conductas de espionaje en las que al autor se lleva el disquete 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 precepto nos remite a los medios o instrumentos descritos en el artículo 197. Como resultado de integrar ambos preceptos, lo prohibido se circunscribe a: 1º El *apoderamiento* de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al secreto; 2º La *interferencia de las telecomunicaciones* de la empresa; y 3º La *utilización de artificios técnicos* de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación. (Conductas que, evidentemente, habrán de realizarse con el ánimo de descubrir un secreto de empresa.)

En suma, se amplía de forma notable el espectro de conductas de espionaje informático que, eventualmente, resultarían 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 relevantes (ej: visualización y memorización de datos

informatizados, sin "apoderamiento" alguno (39) ni empleo de los artificios mencionados en el artículo 197.1; o el descubrimiento casual de la información secreta y posterior comercialización de la misma a competidores). En resumen, pese a lo compleja y farragosa que resulta la descripción de lo prohibido, subsisten lagunas relevantes.

En cuanto a la dimensión subjetiva del tipo, será imprescindible, además del dolo, 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 son, 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., que se refieran al secreto (es decir, ni se precisa que contengan el secreto), o con el empleo de los artificios de reproducción, grabación ..., 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.

La agravación que establece el segundo párrafo para el caso de revelación, divulgación o cesión del secreto, justificada por el efecto expansivo del perjuicio económico, en el marco de la criminalidad informática probablemente encuentre el terreno abonado de aplicación, habida cuenta de la facilidad y rapidez de difusión de la información detectada o descubierta, con un solo gesto y desde el anonimato, a través de las llamadas "autopistas de la información", que conectan telemáticamente a miles de sujetos desde cualquier parte del mundo. Problema distinto –pero común a todos los ilícitos vinculados a la informática– será el de la prueba.

– El artículo 279 se presenta como una versión remozada del artículo 499 anterior, 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 laboral entre sujetos activo y pasivo –como se infiere del artículo 499 VCP–, bastando la obligación legal o contractual de guardar secreto en aquél que lo revela. En la PANCP de 1983, el artículo 277 exigía en el sujeto activo la condición de "empleado" que tuviere encomendada la reserva del secreto, lo cual reducía notablemente el círculo de sujetos activos posibles. En el tema que nos ocupa, esta innovación abre la posibilidad de reprimir algunos hechos hasta ahora 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, directivos y consejeros (ej: un miembro del Consejo representante del capital de una sociedad anónima), que difícilmente realizarían el tipo del artículo 499 VCP, por ausencia de la relación de dependencia (40).

Como en el artículo 278, también se acude en el artículo 279 a la construcción de los delitos de peligro. Basta, para la consumación, que se revele el secreto (cualquiera que sea la forma, lícita o subrepticia, de obtención del mismo), 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.

En cuanto al tiempo límite del deber de guardar secreto, cuestión polémica en nuestros días, el nuevo Código 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 extinguida la relación con la empresa, sólo se cas-

tigará si constituyere delito de competencia desleal" (41).

A la vista de la pena establecida, se considera menos disvalioso el comportamiento cuando el secreto es utilizado en provecho propio. Sin embargo, también constituye una novedad en nuestro Derecho positivo represión de esta conducta, que resultaba impune conforme al Código anterior (si bien cabía aplicar las disposiciones de la Ley de Competencia Desleal) (42).

Se completa esta regulación con el artículo 280 que, como el artículo 279, tampoco contiene referencia específica al espionaje informático, pero podría ser de aplicación a alguna de sus manifestaciones. Al castigar al tercero que no intercepta personalmente el secreto empresarial, y sin embargo lo difunde, revela, cede a terceros o lo utiliza en provecho propio a sabiendas de su origen ilícito, podría servir para incriminar conductas como la difusión, a través de Internet, de noticias, claves, información secreta de distintas empresas, etc., por alguien distinto al *hacker* que hubiera descubierto dicha información. La gravedad de estos hechos, como ya se indicó, a causa del extraordinario efecto expansivo del medio, aconseja intentar su represión. (La conducta del *hacker* sería, en su caso, punible por la vía del art. 278.)

2. Destrucción, modificación o inutilización de archivos y ficheros informatizados con valor económico de empresa (sabotaje informático)

En sentido análogo a la advertencia con que iniciábamos el apartado anterior, también debemos reflejar aquí nuestra discrepancia con los planteamientos que abordan la temática del sabotaje informático como un todo homogéneo, sin adjetivar. Para nosotros, la rúbrica "sabotaje informático" hace referencia exclusivamente a una determinada dinámica comisiva (alteración, supresión o adición 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 se 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 aquélla, 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 del tráfico en una gran ciudad y altera el programa que se ocupa de la ordenación de los semáforos, provocando un caos circulatorio; 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, la 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** (43).

La gama de procedimientos imaginables

para la destrucción o inutilización del *software* resulta amplísima, estimándose que aquéllos 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 para imposibilitar el acceso o utilización de los mismos, introducción de "virus informáticos" o datos erróneos, etc.) (44).

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 conflictoslaborales, 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).

2.1. *Cauces para el sabotaje informático empresarial en el Código anterior*

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). Pues bien: hasta el Código Penal de 1995, donde se contiene referencia específica al sabotaje informático empresarial, el marco legal de referencia para la eventual represión de tales hechos venía conformado, esencialmente, por la normativa penal en materia de daños (arts. 547 y ss. VCP).

– Para los casos de destrucción o inutilización del *software* mediante la actuación directa sobre las instalaciones, edificios o equipos informáticos (*hardware*), o sobre las instalaciones o edificios donde se hallaban aquéllos, cabía aplicar, o bien los artículos 549 a 553 (si el medio comisivo fuese el incendio), o el artículo 563 (previsto como residual y tipo básico), o bien el artículo 554 (delito de estragos). Sobre la aplicación de los primeros, apuntaba CORCOY BIDASOLO (45) el problema suscitado por la evaluación económica del perjuicio. Pues, no se olvide que el legislador establecía la pena en atención al perjuicio irrogado, y dicho perjuicio, según la interpretación más extendida, hacía referencia al deterioro en el valor, intrínseco o en uso, del objeto mismo sobre el que recaía la conducta prohibida, pero no a las consecuencias económicas eventualmente derivadas de ese resultado –innecesarias para el delito de daños, aunque condicionaran su agravación– (46). El tema no era en modo alguno irrelevante cuando se trasladaba 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, siendo así que las penas se graduarían atendiendo sólo al valor del soporte dañado.

El artículo 554 supera el obstáculo anterior, y es por ello que se ha estimado 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.

– Para las conductas proyectadas directamente sobre el *software* (modificación, destrucción o inutilización, por medio de manipulación informática, de programas, archivos, ficheros o datos informatizados), las dificultades para la aplicación de los delitos de daños

tradicionales eran mayores, al menos según la interpretación tradicional, que exigía que el objeto material de los daños consistiera en una cosa ajena, mueble o inmueble, económicamente valorable y susceptible de deterioro, inutilización o destrucción (excluyéndose, pues, las cosas inmateriales). No obstante, estimamos preferible la postura que han defendido, entre otros, GONZALEZ RUS, RUIZ VADILLO, CORCOY BIDASOLO o ROMEO CASABONA (47): Lo verdaderamente relevante en estas figuras es que se deteriore o dañe algo –lógicamente, susceptible de ser deteriorado–, valorable económicamente y que pueda ser objeto del derecho de propiedad. Con lo cual, cabría 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" (48).

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, se reconocía a continuación, en orden a aprehender más ajustadamente el desvalor de muchos de los supuestos de sabotaje informático, la virtualidad de los tipos agravados del artículo 558.5º (para daños provocados "En un archivo, registro, museo, biblioteca, gabinete científico, institución análoga...") y 7º (para los casos de sabotaje en que los perjuicios son de tal entidad que terminan "arruinando al perjudicado").

Con todo, **no llegaba 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, ya habían rechazado la aplicabilidad de las tipicidades clásicas de daños y de sabotaje al "sabotaje informático", regulando, pues, la materia *ex novo*. Por todo ello, unido a la orientación que en la materia venía marcando la comunidad internacional, recomendando a los Estados, desde las distintas instancias, una específica regulación del sabotaje informático (49), **nuestra doctrina penal demandaba también aquí la intervención del legislador,** a fin de otorgar una mayor y mejor cobertura al sabotaje informático (50), "incluso aunque sólo fuera para lograr unas penas más adecuadas al desvalor de estos hechos".

2.2. *El sabotaje informático (empresarial) en el Nuevo Código Penal*

Dentro del Título dedicado a los delitos contra el patrimonio y contra el orden socioeconómico, y en el Capítulo IX ("De los daños"), incluye el legislador de 1995 una referencia expresa al sabotaje informático, en los siguientes términos:

Art. 264.2. "**La misma pena** (prisión de uno a tres años y multa de doce a veinticuatro meses) **se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.**"

Quienes hayan seguido el proceso de reforma penal en nuestro país y su evolución en la comprensión del *computer crime*, habrán, sin duda, detectado, que la disposición aquí transcrita se introdujo en el último de los Proyectos (bastante más tarde que otros ilícitos vinculados a la informática). Esto da idea de la falta de un planteamiento conjunto en torno al tema, rasgo que ha presidido la reforma en este extremo (51).

Según indicábamos al principio del epígrafe, examinamos ahora el sabotaje informático contra intereses de contenido económico. Mas, debemos señalar que, dejando a salvo la referencia a la *alteración* de los datos de carácter personal "en perjuicio del titular... o de un tercero" del artículo 197.2 *in fine*, es

ésta la única modalidad de sabotaje informático que expresamente reconoce el nuevo Código, habida cuenta de la incardinación sistemática de esta figura.

Una lectura más detenida del artículo 264.2 NCP nos lleva a las siguientes conclusiones:

1º En materia de bien jurídico, entendemos que se protegen intereses de contenido económico, pero no necesariamente identificables con el patrimonio stricto sensu. Pese a la exigencia, en el tipo básico de daños (art. 263), de una lesión cuantificable (superior a cincuenta mil pesetas) "en propiedad ajena", y pese a que el primer párrafo del artículo 264 se construye sobre las exigencias deltipo básico, a nuestro juicio, el párrafo segundo de este mismo precepto no precisa tales requisitos. Su diseño es independiente al del tipo básico. (Así, será de aplicación, por ejemplo, a la introducción dolosa de un "virus" en el sistema informático de una entidad bancaria que perturbe el correcto desarrollo de su actividad durante varias jornadas laborales, aunque no conste un perjuicio patrimonial cuantificable.)

2º La descripción de la conducta típica es suficientemente amplia como para abrazar la mayoría de los supuestos de sabotaje informático, se efectúe atentando directamente contra el *software* o contra el *hardware* (como vehículo para lesionar el *software*). Es decir, abrazaría supuestos, por ejemplo, de supresión o alteración de datos informatizados contenidos en el disco duro, pero también a la inutilización de discos, o a la introducción de "virus" en un sistema o en un programa, o a la encriptación de una información de modo que resulte inacesible –e inservible–, etc. En cuanto al resultado, no vemos necesario, según se explicó, la constatación de una lesión patrimonial cuantificable, de modo que bastaría un perjuicio económico difuso (ej: supresión de los archivos informatizados referidos a la cartera de clientes de una compañía de seguros). El objeto material del delito también aparece definido en el nuevo precepto en sentido amplio ("datos, programas o documentos electrónicos", cualquiera que sea el soporte en que se hallen contenidos), de modo que no vemos aquí obstáculos para su eventual aplicación. En relación con los sujetos, el precepto presenta una restricción: el sujeto activo nunca podrá ser el titular de los datos, programas o documentos afectados. Habrán de resolverse, por tanto, fundamentalmente apelando a la legislación en materia de propiedad intelectual, las conductas de aquellos creadores o titulares de programas que introducen ciertas rutinas "autodestructivas" o "virus" para que desplieguen su eficacia en caso de impago, incumplimiento de condiciones contractuales o copia ilícita. La interpretación del elemento normativo "ajenos" va a trasladar al marco del nuevo artículo 264.2 la compleja problemática en torno a la titularidad del *software*.

3º En el tipo subjetivo resulta imprescindible la presencia de dolo. No obstante, no hallamos fundamento para interpretar que el legislador ha pretendido excluir del ámbito de lo punible los supuestos de "sabotaje informático imprudente", en la línea de algunas propuestas doctrinales poco partidarias de la incriminación de cualquier modificación o destrucción de datos o programas por actuaciones descuidadas (52). Bien al contrario, consideramos que estos hechos quedarán subsumidos en el tipo del artículo 267 siempre que la imprudencia sea grave, se ocasionan pérdidas superiores a diez millones de pesetas, y previa denuncia del agraviado. (A la vista de esta configuración delos daños imprudentes, quedan disipados los peligros de un exceso de reacción penal.)

4º No serán infrecuentes, y el propio legislador así lo prevé en el artículo 278.3, las situaciones concursales entre el espionaje informático y las conductas que aquí analizamos (ej: el que descubre la información reservada de una empresa, la altera o hace desaparecer de sus archivos informatizados, o infecta con un "virus informático" el sistema). En estos casos, como se desprende del propio texto legal ("sin perjuicio de las penas..."), serán de aplicación las reglas de concursos.

3. El intrusismo informático (*hacking*) en el Nuevo Código Penal

Con la expresión anglosajona *hacking* (intrusismo informático) se hace referencia a

un conjunto de comportamientos de acceso o interferencia no autorizados –de forma subrepticia– a un sistema informático o red de comunicación electrónica de datos, y a la autilización de los mismos sin autorización o más allá de lo autorizado. Ahora bien: tal delimitación resulta insuficiente, pues, como ya advierte SIEBER (53), el acceso no autorizado puede obedecer a motivaciones muy diversas: puede ser un simple juego, o la respuesta al reto permanente que para el hombre representa la máquina, pero también, en ocasiones se presenta como el *modus operandi* de otro ilícito más grave, ya sea un fraude, sabotaje, etc. Aquí sólo nos ocuparemos de los primeros supuestos, las actuaciones de intrusismo en sentido estricto, despojadas de toda intención de dañar, perjudicar, lucrarse o falsificar... distinta al acceso mismo. Por último, su caracterización y tratamiento penal, lógicamente estará en función de la titularidad de los sistemas informáticos o redes interceptadas y de la naturaleza de los datos o información afectada. (Se comprende que no tendrá la misma entidad la infiltración en un ordenador privado que en los sistemas informáticos del Ministerio de Hacienda, por ejemplo.)

La extraordinaria dimensión que está alcanzado el fenómeno del *hacking* en los últimos tiempos, hasta convertirse en una seria amenaza para los titulares de equipos informáticos –pequeñas y grandes empresas, organismos públicos y entidades privadas, sin distinción–, contrasta con el escaso interés que ha despertado en el mundo jurídico. Para la corriente mayoritaria, tales conductas carecen de entidad suficiente para merecer la intervención del Derecho Penal: o bien se materializan en otro hecho más grave (y ya estarian castigadas por la vía del fraude, espionaje, sabotaje informático, etc.), o, caso contrario, resultan inofensivas, y su incriminación atentaría contra el principio de lesividad y el de intervención mínima (estaríamos castigando, como mucho, actos preparatoriosde no se sabe qué delito). A nuestro entender, en cambio, el tema se ha simplificado en exceso, hurtándose un debate más serio, con el bien jurídico como telón de fondo. Sin insistir ahora en argumentos detallados en otro lugar (54), recordaremos, únicamente, la conveniencia de distinguir dos niveles:

– Primero, cualquier conducta de intrusismo informático supone una agresión contra el interés del "titular" o "propietario" del sistema o de la información interceptada. (Interés individual en mantener la integridad, la reserva, de aquello que le pertenece en exclusividad; al margen del contenido de la información almacenada o tratada en el sistema informático afectado.) Proteger al "propietario" (en sentido atécnico) en el pacífico disfrute de su "propiedad" frente a agresiones y perturbaciones externas no autorizadas, constituye una opción legislativa, desde luego. Pero será tan conforme o tan contrario al principio de intervención mínima como, por ejemplo, el delito de allanamiento de morada, o el de reciente incorporación al Código Penal en el artículo 203 (allanamiento de domicilio de persona jurídica, despacho profesional, etc.).

– En un segundo plano situaríamos el intrusismo en sistemas o equipos informáticos particularmente relevantes, por razón del contenido de la información que procesan o almacenan (información catalogada como "sensible") y por las funciones que tienen asignadas en el seno de las relaciones jurídicas, económicas y sociales. A nuestro entender, el *hacking* sobre estos "sistemas sensibles" está afectando gravemente a un interés supraindividual o colectivo, que podríamos denominar "seguridad informática", interés de difícil aprehensión y definición, debido a su carácter difuso e inmaterial, pero cuya existencia todos constatamos. La "seguridad informática" constituye hoy un ingrediente indispensable para el normal desarrollo de las relaciones del tráfico, y se tambalea peligrosamente cuando se ve afectada por las conductas de los *hackers*. (Pensemos, a modo de ejemplo, la desconfianza que generaría en las transacciones y transferencias electrónicas de fondos realizadas, el que saliera a la luz pública que el Sistema Nacional de Compensación Electrónica hubiera sufrido infiltraciones externas y que estaba siendo utilizado por un grupo de jóvenes para enviarse mensajes. ¿No resultaría afectado ese interés colectivo al que nos

referimos, al margen de los perjuicios económicos que se hubieren irrogado?) Plantear en esta sede una adecuada tutela penal autónoma frente al intrusismo informático, entendemos que no puede considerarse "un exceso de reacción penal" y merece, por lo menos, un debate en profundidad.

3.1. Hacking *y delincuencia patrimonial en el viejo Código Penal*

Ciñéndonos, nuevamente, al ámbito de los delitos patrimoniales y socioeconómicos en el marco del viejo texto punitivo, lo cierto es que, tanto la infiltración sin autorización en un sistema informático como el llamado "hurto de tiempo" de máquina, resultaban impunes con carácter general, siempre que no pudieran reconducirse –con los problemas de interpretación ya apuntados– por las vías que anteriormente sugerimos respecto al espionaje informático o sabotaje informático. (El único cauce autónomo posible se hallaba en el antiguo artículo 135 bis a, susceptible de ser aplicado, por su amplia formulación, al acceso sin autorización a sistemas de procesamiento de información relativa a la defensa nacional o seguridad nacional. Mas, por razones de bien jurídico, no interesa su examen al presente estudio.) Las infiltraciones subrepticias en las comunicaciones electrónicas de datos, en cambio, hubieran podido encontrar encaje en el artículo 497 bis anterior, si bien con las reservas que comentamos. En la sede de los delitos patrimoniales, en todo caso, no aparecía disposición alguna aplicable a las conductas de hacking que afectaran a la información con valor económico empresarial. Pero tampoco nuestra doctrina echaba en falta dicha normativa (55).

3.2. *La represión del* hacking *en el Nuevo Código Penal*

Dentro del Título dedicado a los delitos contra el patrimonio y contra el orden socioeconómico, el Código de 1995 ha introducido una figura de nuevo cuño orientada a reprimir algunas manifestaciones de intrusismo informático. Incardinado en la Sección "De las defraudaciones de fluido eléctrico y análogas", el artículo 256 dispone: **"El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses".**

Tenemos que admitir, de partida, las dificultades que encontramos para interpretar el alcance de esta figura (a falta de antecedentes, a falta de cualquier justificación del legislador y a falta, por último, de todo apoyo doctrinal o jurisprudencial), dificultades que se agravan cuando intentamos coordinar su contenido con las previsiones relativas al sabotaje informático, comentadas en el epígrafe anterior. Apuntaremos, no obstante, alguna reflexión:

– Parece claro que la mente del legislador no albergaba profundos planteamientos sobre "un nuevo bien jurídico" supraindividual, como la "seguridad informática" o similar, digno de tutela. La incardinación sistemática del artículo 256 y la exigencia de un perjuicio patrimonial cuantificable así lo delata. Y es claro, asimismo, que tampoco se pretendió procurar una protección *integral* del titular de la información o de los equipos informáticos frente a cualquier acto de intrusismo o perturbación exterior. Se ha optado, a nuestro entender, por una forma de tutela *parcial* al titular de los equipos informáticos: sólo ante las conductas denominadas "hurto de tiempo de la máquina". Y ni siquiera ante todas éstas, sino sólo ante las que ocasionan un perjuicio patrimonial cuantificable superior a cincuenta mil pesetas.

– En consecuencia, el bien jurídico tutelado es el patrimonio individual (el patrimonio del titular de los equipos informáticos), que ha de sufrir esa disminución material. Sujeto activo puede serlo cualquiera: tanto los empleados (que utilizan los ordenadores más allá de lo autorizado) como los terceros (que, infiltrándose a distancia o de forma subrepticia en las propias instalaciones, usan los ordenadores sin autorización). La conducta típica excluye, entendemos, el castigo del mero acceso a un

sistema, tras descubrir su puerta falsa, sin permanencia posterior en el mismo. Mas, habiéndose diseñado la figura del artículo 256 como un delito de resultado material, se limitan notablemente sus posibilidades. Pues, si los perjuicios se hubieran ocasionado sobre el *hardware*, serán de aplicación los delitos de daños; caso de afectar al *software*, se habrá de acudir a la nueva disposición del artículo 264.2 (siempre que exista dolo, incluso eventual). ¿Qué queda, pues, para el artículo 256? Perjuicios que consistan en perturbaciones, molestias, alteraciones en el correcto funcionamiento del sistema o la obstaculización del uso legítimo a quienes estuvieren autorizados al efecto. La dificultad mayor estriba en que todos esos perjuicios son difícilmente aprehensibles y cuantificables. Además, si no afectan al titular, sino a terceros, no se computan a tenor de este precepto. Finalmente, la exigencia de dolo en la dimensión subjetiva del tipo (dolo que ha de abarcar también la provocación del perjuicio) restringe de modo definitivo su contenido, anulando casi por completo su virtualidad en el ámbito del intrusismo informático que aquí examinamos, donde falta, precisamente, dicha intención.

REFLEXION FINAL

A modo de conclusión final, y tras este rápido recorrido, quisiéramos apuntar:

1º Probablemente, las disposiciones comentadas están llamadas a desempeñar, en muchos casos, un mero papel testimonial, habida cuenta de las características de la criminalidad informática, y las dificultades que plantea su detección y prueba. Con todo, nuestra valoración inicial es positiva, desde la perspectiva de la función de motivación de la norma penal.

2º Hemos examinado *sólo* algunos aspectos de la delincuencia vinculada al ordenador en el nuevo Código. Pero, como ya insinuamos con anterioridad, suverdadero alcance en esta materia sólo se entenderá examinando otras figuras –aquí no estudiadas– cuya formulación típica no impide la "entrada" de las nuevas tecnologías (con lo cual, cabría su aplicación a ilícitos sobre o mediante elementos informáticos: fraude fiscal, delitos contra la Seguridad Social, blanqueo de capitales, delitos societarios...).

3º Por último, es de lamentar que se haya perdido la incomparable oportunidad de una reforma penal global para abordar los problemas del computer crime de una forma completa y sistemática, colofón de un debate doctrinal en profundidad.

NOTAS

(1) Vid. GUTIERREZ FRANCES, M.: *Fraude informático y estafa*. Ministerio de Justicia. Madrid. 1991. pág. 88 y ss.

(2) Basta un repaso por los informes nacionales presentados al Congreso de la AIDP sobre "Computer Crimes and Other Crimes against Information Technology" en Würzburg, en octubre de 1992, recogidos en la *International Review of Penal Law*, vol. 64, 1993, *passim*.

(3) Cfr. DEVEZE, J.: "Commentaire de la Loi núms. 88-19 du 5 janvier 1988 relative a la fraude informatique". *Lamy droit de l'informatique*, vol. 26, núm. 1, 1988, pág. 6 y ss.

(4) Vid. GUTIERREZ FRANCES, M.: "En torno a los fraudes informáticos en el Derecho español". Actualidad Informática Aranzadi, nº 11, Ed. Aranzadi, Madrid, abril, 1994, pág. 7 y ss.

(5) Más ámpliamente en GUTIERREZ FRANCES, *Fraude informático...*, cit., pág. 90 y ss.

(6) CORCOY BIDASOLO, M., JOSHI, U.: "Delitos contra el patrimonio cometidos por medios informáticos". Separata de la *Revista Jurídica de Cataluña*, núm. 3, 1988, pág.. 142.

(7) *Ibidem*, pág. 142; en el mismo sentido, GONZALEZ RUS, J.J.: "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", *Poder Judicial*, núm. especial IX, Madrid, 1989, pág. 160.

(8) ROMEO CASABONA, C.M.: *Poder Informático y Seguridad Jurídica*, Ed. Fundesco, Madrid, 1987, pág. 75 y ss.; CORCOY, JOSHI, "Delitos contra el patrimonio...", cit., pág. 138 y ss.

(9) GARCIA-PABLOS MOLINA, A.: "El impacto de las tecnologías y medios de información en el Derecho penal", Boletín CITEMA, núm. 118, 1985, pág. 66.

(10) GUTIERREZ FRANCES: "En torno a los fraudes...", cit., pág. 9.

(11) Recordemos que en este contexto no se computan las actuaciones ilícitas concernientes a las tarjetas con banda magnética como delitos informáticos, YAMAGUCHI, A., "Computer Crimes and Other Crimes against Information Technology in Japan", *International Review of Penal Law*, vol. 64, cit., pp. 434 y ss. La legislación canadiense, por ejemplo, se ocupa de todas las conductas ilícitas o abusivas relacionadas con las tarjetas de crédito conjuntamente (artículo 301.1 C.P. canadiense).

(12) El estado de la cuestión hasta el presente en España, en PREGO DE OLIVER Y TOLIVAR, A., "Problemas penales de la tarjeta de crédito", *Cuadernos de Derecho Judicial, La Nueva Delincuencia II*, Consejo General del Poder Judicial, Madrid, 1994, pág. 11 y ss.

(13) Postura de la Fiscalía General del Estado, en Consulta 2/88, *Memoria Anual de la Fiscalía General del Estado*, 1989, pág. 521 y ss.

(14) BACIGALUPO ZAPATER, E.,"Utilización abusiva de cajeros automáticos por terceros no autorizados", *Poder Judicial, núm. especial IX*, Madrid, 1989, pág. 85 y ss.

(15) DE LA MATA, N.J.: "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante tarjeta sustraída a su titular". *Poder Judicial*, núm. especial IX. Madrid, 1989, pág. 159 y ss.; GUTIERREZ FRANCES, *Fraude informático...*, cit., pág. 470 y ss.

(16) Cfr. GUTIERREZ FRANCES: "En torno a los fraudes...", cit., pág. 10, (nota 28).

(17) GUTIERREZ FRANCES, *Fraude informático...*, cit., págs. 582-587, 604 y ss., acogiendo el planteamiento de GOMEZ BENITEZ, J.M.: "Función y contenido del error en el tipo de estafa", *ADPCP*, 1985, pág. 335 y ss.

(18) GONZALEZ RUS, J.J.: *Los intereses económicos de los consumidores. Su protección penal*, Instituto Nacional de Consumo, Madrid, 1986, pp. 265 y ss., defiende esta solución, que, a nuestro juicio, no es compatible con su entendimiento de la estafa y con sus conclusiones respecto a las defraudaciones mediante ordenador, en "Tratamiento penal de los ilícitos patrimoniales...", cit.,pág., 48 y ss.; BAJO FERNANDEZ, *Manual de Derecho Penal*, P.E., vol. II, 2ª ed., Centro de Estudios Ramón Areces, Madrid, 1993, pág. 300.

(19) DE LA MATA, "Utilización abusiva...", cit., página 151 y ss.

(20) Más extensamente en, DE LA MATA: "Utilización abusiva...", cit., pág. 159 y ss. También, GUTIERREZ FRANCES: *Fraude informático...*, cit.,pág. 461 y ss.

(21) Vid. en GUTIERREZ FRANCES: *Fraude informático...*, cit., pág. 472-474, la disparidad de soluciones que para la doctrina tienen estos supuestos.

(22) Vid. ROMEO CASABONA, C.M.: *Poder Informático...*, cit., pág. 168-170. Sobre la distinción entre "información" y "datos", vid. PIRAGOFF, D.K., "Computer Crimes and Other Crimes Against Information Technology in Canada", *International Review of Penal Law*, AIDP, vol. 64, 1993, páginas 210-211.

(23) MARBRACH, W.D., KASINDORF, M., SANDZA, R.: "Was It Really War Games?", *Newsweek*, vol. 106, 1985, pág. 23.

(24) Publicado en EL PAIS, de 10 de enero de 1990, pág. 26.

(25) Por todos, SIEBER, U., *The International Handbook on Computer Crime*, John Wiley and Sons, Chichester, 1986, pág. 12 y ss.

(26) 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, pág. 512.

(27) En Alemania, cfr. MÖHRENSCHLAGER, M.: "Computer Crimes and other Crimes against Information Technology in Germany", *International Review of Penal Law*, *AIDP*, vol. 64, 1993, pág. 344 y ss.; VASSILAKI, I.: "Computer Crimes and Other Crimes against Information Technology in Greece", *International Review...*, ult. cit., pág. 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 Technology in Austria", *International Review...*, ult. cit., pág.141 y ss.

(28) GONZALEZ RUS: "Tratamiento penal de los ilícitos patrimoniales...", cit., pág. 43.

(29) 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 ss. de dicha Ley, regimen parcialmente modificado por la 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 constituían los artículos 534 bis a) y ss. del viejo CP., introducidos por la reforma penal de 11 de noviembre de 1987, donde se abandonó, al menos formalmente, la técnica de la "ley penal en blanco".

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

(31) Vid. el comentario al planteamiento del Tribunal Supremo en, BAJO FERNANDEZ, M.: *Manual de Derecho Penal*, P.E., vol. II, 2ª ed., cit., pág. 377.

(32) GONZALEZ RUS: "Tratamiento penal de los ilícitos patrimoniales...", cit., pág. 45; en el mismo sentido, MORALES PRATS: *La tutela penal de la intimidad...*, cit., p. 203.

(33) Vid., más ampliamente en, GUTIERREZ FRANCES, M.: "Notas sobre la delincuencia informática: atentados contra la información como valor económico de empresa", *Estudios de Derecho Penal Económico*, núm. 18, (Ed. ARROYO ZAPATERO, TIEDEMANN), Universidad de Castilla-La Mancha, Cuenca, 1994, pág. 187 y ss., y bibliografía allí citada.

(34) JORGE BARREIRO: "Descubrimiento y revelación de secretos. Un estudio de Derecho Penal español", *RDP*, núm. 67, 1982, pág. 253.

(35) Vid. MORALES PRATS: "Problemática jurídico-penal...", cit., pág. 362, rechazando la aplicabilidad del artículo 497 bis para los supuestos en que se interfiere una transmisión informática de datos.

(36) Cfr. GUTIERREZ FRANCES: "Notas sobre la delincuencia...", cit., pág. 191-193 y nota (30).

(37) 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), núm. 2, Ministerio de Justicia, 1983, pág. 737 y ss.

(38) 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., cit., página 364 y ss.

(39) Vid. MORALES PRATS: "Problemática jurídico-penal...", cit., pág. 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).

(40) Vid. BAJO FERNANDEZ: *Manual de Derecho Penal*, P.E., V. II, 2ª ed., cit., pág., 380.

(41) BAJO FERNANDEZ: ult. cit., pág. 382.

(42) GUTIERREZ FRANCES: "Notas sobre la delincuencia...", cit., pág. 192.

(43) Más extensamente en, GUTIERREZ FRANCES: ult. cit., pág. 199 y ss.

(44) CORCOY BIDASOLO, M.: "Sabotaje informático", *Textos de ponencias y comunicaciones. Congreso sobre Derecho Informático*, Facultad de Derecho de Zaragoza, junio, 1989, pág., 543 y ss., donde recoge un extenso listado de modalidades comisivas y técnicas de sabotaje informático.

(45) CORCOY BIDASOLO: ult. cit., pág. 558.

(46) BAJO FERNANDEZ: Manual de Derecho Penal, P.E., vol. II, 2ª ed., cit., pág. 508.

(47) CORCOY BIDASOLO: "Sabotaje informático", ult. cit.; GONZALEZ RUS: "Tratamiento penal de los ilícitos patrimoniales...", cit., pág. 47; ROMEO CASABONA: "Delitos patrimoniales en conexión...", cit., pág. 516-517; RUIZ VADILLO, E.: "Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad eco-

nómica", *Poder Judicial*, núm. especial IX. CGPJ, Madrid, 1989, pág. 60.

(48) GONZALEZ RUS: "Tratamiento penal de los ilícitos patrimoniales...", cit., pág. 47; también CORCOY BIDASOLO: "Sabotaje informático", cit., pág. 559 y ss.

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

(50) ROMEO CASABONA: *Poder Informático...*, cit., página 178.

(51) En Alemania, por el contrario, la Segunda Ley de Lucha contra la Criminalidad Económica, de 15 de mayo de 1986 fue precedida de un amplio y profundo debate. Cfr. MÖHRENSCHLAGER, M.: "Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG)", *Wistra*, 4, 1986, pág. 123 y ss.; ACHENBACH, H., "Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität", *Neue Juristische Wochenschrift*, 30, 1986, pág. 1835 y ss.

(52) ROMEO CASABONA, C.M.: "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", *Poder Judicial*, núm. 31, CGPJ, Madrid, septiembre, 1993, págs. 203-204.

(53) Un recorrido por el Derecho comparado y la manera de afrontar el intrusismo informático en las distintas legislaciones en, SIEBER, *The International Handbook...*, cit., págs. 86-90.

(54) Más extensamente en GUTIERREZ FRANCES, M.: "El intrusismo informático (*hacking*): ¿represión penal autónoma?", *Informática y Derecho*, Universidad Nacional de Educación a Distancia, Mérida, 1995 (en prensa).

(55) Vid. ROMEO CASABONA, "Tendencias actuales...", cit., pág. 204.