

# Delitos Informáticos de carácter patrimonial

CARLOS M. ROMEO CASABONA

*Catedrático de Derecho Penal. Universidad de La Laguna*

## 1. Introducción

La incorporación de la tecnología informática también al mundo empresarial y económico ha abierto un nuevo campo a la delincuencia de índole patrimonial, quizá no tan llamativo como los atentados a la intimidad personal y demás derechos fundamentales del individuo conectados con las bases de datos públicas o privadas, pero de una innegable trascendencia para el normal desenvolvimiento del tráfico económico<sup>1</sup>. Aparte de los diversos problemas que presenta la manifestación de esta nueva delincuencia (entre los que se encuentra, en primer lugar, la difícil detección de esta clase de atentados, al ampararse sus autores precisamente en las características tecnológicas de los medios informáticos), están otros de índole técnico-jurídica, concretamente en que en ocasiones resulta problemático encuadrar estas conductas en los delitos tradicionales contra el patrimonio, si no se quieren vulnerar las garantías que se derivan de la vigencia del principio de legalidad en nuestro sistema jurídico. Las conductas más significativas desde esta perspectiva podrían agruparse en estas cuatro modalidades principales: a) manipulaciones de datos y/o programas, o 'fraude informático'; b)

- 1 Me baso fundamentalmente en mi trabajo anterior *Poder Informático y Seguridad Jurídica*, Fundesco, Madrid, 1988, 35 y ss., debidamente actualizado. V. con carácter general en la bibliografía española, Mirentxu CORCOY y Ujala JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, en "Revista Jurídica de Catalunya", 133 y ss. (1988); Juan José GONZALEZ RUS, *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, en "Revista de la Facultad de Derecho de la Universidad Complutense de Madrid", monográfico nº 12, 107 y ss. (1986), el mismo, *ratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, en "Poder Judicial", nº Especial IX, 39 y ss. (1989); M<sup>º</sup> Luz GUTIERREZ FRANCÉS, *Fraude informático y estafa*, Centro de Publicaciones del Ministerio de Justicia, Madrid, 1991, *passim*; Enrique RUIZ VADILLO, *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica*, en "Poder Judicial", nº Especial IX, 53 y ss. (1989).

copia ilegal de programas; c) obtención y utilización ilícita de datos, o 'espionaje informático'; d) destrucción o inutilización de datos y/o programas, o 'sabotaje informático'; e) agresiones en el *hardware* o soporte material informático, principalmente 'hurto de tiempo del ordenador'<sup>2</sup>. Esta clasificación responde, según indica SIEBER<sup>3</sup>, no sólo a un criterio sistematizador vinculado a las características del procesamiento automático de datos, sino al mismo tiempo a una separación de diversos tipos criminológicos de conducta. Veamos brevemente cada una de ellas.

Como ya he adelantado, el hilo conductor implícito en toda la discusión que se propone a continuación radica en la trascendente cuestión de si los tipos penales actuales que van a ser objeto de examen permiten una interpretación extensiva, basada en una visión evolutiva o progresiva de los mismos, de forma que las conductas a las que dedicamos nuestra atención queden abarcadas por esos tipos delictivos, o, si por el contrario, estamos incurriendo en analogía perjudicial para el reo, contraria a uno de los basamentos irrenunciables del Derecho penal español, como es el principio de legalidad de los delitos, si se trata efectivamente tan sólo de 'hechos semejantes'<sup>4</sup>.

En derecho comparado encontramos el correspondiente reflejo de la preocupación existente porque las conductas dolosas que hemos agrupado en torno a las agresiones realizadas contra medios o sistemas informáticos o a través de los mismos queden cubiertas por la ley penal sin ninguna concesión a posibles lagunas punitivas. La OCDE, en su estudio sobre los aspectos penales de la criminalidad económica perpetrada en conexión con ordenadores, ha recomendado en esta dirección a los países miembros de dicha organización el aseguramiento de la punición, incluso por medio de iniciativas legislativas, de la mayor parte de los comportamientos que estamos tratando<sup>5</sup>.

Algunos países han tomado iniciativas en este sentido, incluyendo nuevos tipos penales específicamente referidos a conductas relacionadas con agresiones en conexión con sistemas informáticos, lo que hace pensar que los tipos penales tradicionales relacionados con aquéllas no satisfacían plenamente en sus objetivos protectores. Las diversas reformas se podrían agrupar en dos técnicas

- 2 Clasificación que fue propuesta por LAMPE y posteriormente asumida por SIEBER (indiscutible primer especialista europeo en la materia) en su obra capital. V. Ernst-Joachim LAMPE, *Die strafrechtliche Behandlung der sog. Computer-Kriminalität*, en "Goldammer's Archiv für Strafrecht", 1 y ss. (1975); Ulrich SIEBER, *Computerkriminalität und Strafrecht*, 2a ed., Köln 1980, 39 y s.
- 3 SIEBER, *lug. cit.*
- 4 A este respecto, no parece decisivo el concepto de autor del que se parta, pues siempre será necesario que él mismo o su "instrumento" (persona o cosa) realicen la acción típica. V., sin embargo, CORCOY/JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 136.
- 5 V. OECD, *Computer Related Crime: Analysis of Legal Policy*, París 1986.

legislativas principales: la primera consiste en la creación de 'tipos de equivalencia', es decir, introducción de nuevos tipos penales que complementen a los ya existentes corrigiendo en la descripción de la acción típica las carencias detectadas en aquéllos (p. ej., en lo relativo a los modos o formas de realización de la acción y en el objeto material de la misma). Presenta la ventaja de concreción del tipo y vinculación a bienes jurídicos merecedores de protección penal muy bien perfilados, lo que es estimable en aras de la seguridad jurídica; pero su contrapartida consiste en que es fácil incurrir en excesivo casuismo o prolijidad, a la vez que se corre el riesgo de dejar sin cobertura determinadas conductas dignas de la intervención penal y otras nuevas que se pongan en práctica al hilo de los constantes avances tecnológicos en este sector. El otro procedimiento consiste básicamente en la descripción de conductas normalmente peligrosas para el correcto funcionamiento de los sistemas informáticos y sus diversos componentes, esto es, se protege aquél y éstos en cuanto tales por la potencialidad de producir una lesión a ciertos bienes jurídicos. Junto con la ventaja de asegurar una amplia cobertura penal frente a conductas indeseables, presenta el inconveniente de la pérdida de perspectiva de los bienes jurídicos que se desean proteger y de conferir una protección tal vez excesiva en este campo, lo que supone, respectivamente, riesgos para la seguridad jurídica y de sobrepasar el principio de intervención mínima al que ha de ceñirse el Derecho Penal en su concepción actual. Una reforma penal en nuestro país (en general en relación con la delincuencia vinculada a las modernas tecnologías de la información), debería tener en cuenta, en mi opinión, estas observaciones, aunque en principio me inclino a favor de la primera de las dos técnicas citadas, por ser mayores sus ventajas que sus inconvenientes y poder ser evitados éstos con cuidadosa redacción de los tipos penales.

Como ejemplo de la primera vía, citemos en primer lugar, el Código Penal alemán<sup>6</sup>. En Portugal la reforma del Código penal culminada en 1982 ha introducido en su sistema punitivo varias infracciones delictivas relacionadas con la informática, que se aproxima al modelo alemán<sup>7</sup>. En la misma línea se sitúan el Código Penal austriaco y Canadá, donde también se reformó el Código Penal en 1985<sup>8</sup>. Un ejemplo de la segunda opción legislativa lo encontramos en

■ 6 En la *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität*, promulgada el 15 de mayo de 1986 y en vigor desde el 1º de agosto del mismo año.

■ 7 No ha de extrañar que se le califique de modelo, puesto que aunque la reforma alemana se aprobó varios años más tarde que la portuguesa, aquélla venía siendo objeto de debate parlamentario y doctrinal públicos ya en la década de los setenta.

■ 8 *Criminal Law Amendment Act*, de 20 de junio de 1985. Como ejemplo de técnica legislativa en el sistema anglosajón se incluye el texto de la Section 387 (1.1): "Comete daños quien voluntariamente a) destruye o altera datos; b) hace ininteligibles, inútiles o inefectivos datos; c) obstruye, interrumpe o interfiere el uso legal de datos; o d) obstruye, interrumpe o interfiere a una persona en el uso legal de datos o deniega el acceso a datos a una persona que esté autorizada para ello". La pena no será superior a diez años (Sect. 387. 5). V. al respecto, D.K. PIRAGOFF, *Combatting Computer Crime with Criminal Laws*, en H.W.K. Kasperen (ed.), "Strafrecht in de Informatiemaatschappij", Amsterdam 1986, 110.

Francia, por medio de una todavía reciente Ley de modificación del Código Penal en materia de delincuencia vinculada con las nuevas tecnologías de la información<sup>9</sup>. En los Estados Unidos, los Estados federados han introducido también en sus respectivos Códigos Penales nuevos delitos relativos a la delincuencia vinculada a sistemas informáticos; y, como competencia federal, el *United States Code* incluye un catálogo más reducido de delitos<sup>10</sup>.

De todas formas, una hipotética revisión del Código Penal en relación con las conductas analizadas en este trabajo debería realizarse en el contexto de una reforma más amplia atenta a la incidencia de las nuevas tecnologías de la información en ciertos bienes jurídicos que podrían ser lesionados sin que los hechos se adecuen a los tipos respectivos existentes en la actualidad, lo cual parece necesario y corrobora la nutrida actividad legislativa de otros países de nuestro mismo entorno jurídico-cultural, como he manifestado en otro lugar<sup>11</sup>. Por otro lado, debe afrontarse en una confección de un Código Penal de nueva factura, necesidad inaplazable que es sentida de forma unánime por la doctrina, pues es la única manera de lograr una unidad de perspectiva y de coherencia en un Código como el actual que, arrancando en sus cimientos de 1848, ya no se reconoce a sí mismo. A ello pretende dar respuesta el Proyecto de CP 1992, y en concreto, con la incorporación de algunas figuras delictivas nuevas relacionadas con esta materia, que serán objeto de comentario más abajo, al igual que ya he realizado más arriba con las correspondientes en relación con la protección penal de la intimidad.

Por último, no hay que olvidar una importante reflexión muy repetida y sabida, y es que los instrumentos jurídicos son una vía para la protección de los bienes jurídicos, pero no la única ni la más eficaz. Para prevenir estas conductas parece más eficaz apostar por la adopción de medidas de seguridad y de protección materiales, tecnológicas (valiéndose de procedimientos informáticos) y laborales, en su caso, en intensidad proporcional al valor intrínseco de los sistemas informáticos que se posean y de su importancia operativa para el funcionamiento de la empresa, entidad o administración pública afectadas<sup>12</sup>.

■ 9 Ley nº 88-19 de 5 de enero de 1988. V. Michèl VIVANT (ed.), *Lamy Droit de L'Informatique*, Paris, 1989, 1505 y ss.

■ 10 *Counterfeit Acces Device and Computer Fraud and Abuse Act*, en vigor desde el 12 de octubre de 1984.

■ 11 V. al respecto más extensamente, ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, cit., 32 y ss., 106 y ss., 137 y s. y 172 y s.

■ 12 V. sobre el particular, Thomas FISCHER, *Computer-Kriminalität. Gefahren und Abwehrmassnahmen*, P. Haupt, Bern 1979, 29 y ss.; Michele M. CORRERA/ Pierpaolo MARTUCCI, *I reati commessi con l'uso del computer*, Cedam, Padova, 1986, 46 y ss.; Thomas DEHN/Werner PAUL, *Vorbeugung bei Computerviren*, en "Computer und Recht" (1989), 70 y s.

## 2. Manipulación de datos informatizados

La manipulación de datos informatizados constituye la forma más frecuente de aparición del llamado delito informático en las sociedades de alto desarrollo tecnológico y forman también el núcleo del mismo desde un punto de vista criminológico<sup>13</sup>.

La manipulación consiste en la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero<sup>14</sup>. Constituyen lo que se conoce como *fraude informático*. Las manipulaciones recaen por lo general en modificaciones de la contabilidad de la empresa, de facturaciones de bienes, relación de pagos de salarios, pensiones o ayudas sociales y retenciones vinculadas con los mismos, estado y movimiento de cuentas de clientes bancarios, intereses de los mismos, balances, inventarios, etc. Tales alteraciones pueden producirse, como decía, en las distintas fases en que puede ser dividido el manejo de los datos: a) en la entrada o introducción de los mismos en el programa correspondiente, o 'input' ; b) en el programa mismo; y, c) en la salida de los datos, o 'output' , una vez procesados convenientemente por el ordenador. Las tres modalidades de manipulación han encontrado su correspondiente reflejo en la realidad. De todas formas, algunas de ellas pueden realizarse de forma distinta, como son las manipulaciones a distancia con la ayuda de la telemática y las efectuadas en cajeros bancarios automáticos, valiéndose para ello de las llamadas tarjetas de crédito, cuando están provistas de una banda magnética.

### 2.1. Su encuadre en los tipos delictivos patrimoniales del Código penal vigente.

La peculiaridad del medio empleado en las manipulaciones de datos informatizados, el hecho de que en realidad la acción recaerá sobre elementos incorpóreos e intangibles (recuérdese, p. ej. la Transferencia Electrónica de Fondos), y de que no se actúa directamente sobre personas sino sobre máquinas, plantea la dificultad del encuadre o adecuación de estas conductas en los tipos delictivos contra el patrimonio correspondientes. Con tal fin, vamos a proceder a continuación a un análisis dogmático de los tipos penales patrimoniales

■ 13 V., en este sentido, LAMPE, *Die strafrechtliche Behandlung der sog. Computer-Kriminalität*, cit., 2; Donn B. PARKER, *Fighting Computer Crime*, New York 1983, *passim*.

■ 14 ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, cit., 47. El ánimo de lucro es el elemento diferenciador de manipulaciones conectadas con bienes jurídicos diferentes. V. otras definiciones, p. ej., Wolfgang STEINKE, *Kriminalität durch Beeinflussung von Rechnerabläufen*, en "Neue Strafrechtzeitschrift", 295 (1984).

de enriquecimiento más significativos recogidos en el Código penal vigente español, comparándolos con las modalidades más problemáticas de manipulaciones de datos informatizados<sup>15</sup>.

### 2. 1.1. El delito de hurto

El objeto en el que recae la acción, en el delito de hurto, ha de ser una *cosa mueble ajena*, lo que implica analizar el concepto de cosa (mueble)<sup>16</sup>. Ha de tratarse de cosas corporales, en las que sea posible su aprehensión o apoderamiento material, quedando excluidas las incorporales o inmateriales. Trasladada esta apreciación a las manipulaciones del llamado dinero contable, escritural o documental, por medio de ordenadores, la conclusión lógica es que no caben estos delitos aplicados a las mismas: en estos casos se está actuando sobre cosas inmateriales, se trata no de una cosa material (dinero en metálico), sino de un derecho de crédito en favor de su titular. A la misma conclusión podemos llegar cuando lo que se sustrae por este procedimiento son bienes que se facturan a un cliente ficticio, siempre que no se produzca una aprehensión material de los mismos por el autor del hecho. Por estas razones, el delito de hurto no ofrece de *lege lata* los medios adecuados para la represión penal de estas manipulaciones realizadas con ánimo de lucro<sup>17</sup>.

Un comportamiento semejante es el de la utilización de tarjetas de terceros sin su consentimiento provistas de banda magnética en cajeros automáticos con el fin de obtener dinero en metálico. Hace ya tiempo<sup>18</sup> que he apuntado que el hecho es subsumible en los delitos de apoderamiento, en concreto en el delito de hurto, pero transformado en el de robo con fuerza en las cosas por la

- 15 Sobre lo que sigue, v. más ampliamente ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, cit., 47 y ss.
- 16 V. por todos sobre la cuestión en Derecho español, GONZALEZ RUS, *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, cit., 130 y ss.
- 17 De esta opinión, GONZALEZ RUS, *Aproximación al tratamiento penal de los ilícitos patrimoniales*, cit., 133 y ss. En la literatura alemana, Rainer von zur MÜHLEN/ Rainer SCHOLTEN, *Computer-Manipulationen aus strafrechtlicher Sicht*, en "Neue Juristische Wochenschrift", 1642 (1971); SIEBER, *Computerkriminalität*, cit., 198; de opinión contraria, STEINKE, *Kriminalität durch Beeinflussung von Rechnerabläufen*, cit., 297. En Francia, la jurisprudencia considera el dinero contable (*monnaie scripturale*) como "entrega en metálico"; v. por todos, Jean PRADEL/ Christian FEUILLARD, *Les infractions comises au moyen de l'ordinateur*, en "Revue de Droit Pénal et de Criminologie", 311 (1985).
- 18 V. Carlos M. ROMEO CASABONA, *La utilización abusiva de tarjetas de crédito*, en "Revista de Derecho Bancario y Bursátil", nº 26, 303 y ss. (1987), y en "Actualidad Penal", nº 39, 1825 y ss. (1987); el mismo, *Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos*, en "Poder Judicial" nº especial IX, 109 y ss. (1989). V. sobre esta materia también, Enrique BACIGALUPO ZAPATER, *Utilización abusiva de cajeros automáticos por terceros no autorizados*, en últ. lug. cit., 85 y ss.; Luis Román PUERTA LUIS, *Las tarjetas de crédito en el campo penal*, últ. lug. cit., 97 y ss.; Cándido CONDE-PUMPIDO TOURÓN, *Las tarjetas de crédito como instrumento para la comisión de un delito: dos sentencias*, últ. lug. cit., 133 y ss.; Antonio GIL MARTINEZ, *Algunos supuestos delictivos de tarjetas de crédito y cajeros automáticos*, últ. lug. cit., 141 y ss.; Norberto J. de la MATA, *Utilización abusiva de cajeros automáticos: apropiación de dinero mediante tarjeta sustraída a su titular*, últ. lug. cit., 151 y ss.

utilización de llaves falsas (art. 504 nº 4º CP), al estimar que la tarjeta es en sí misma (o, mejor: cumple la función de) una 'llave', en el sentido del art. 510 nº 2º CP<sup>19</sup>.

### 2.1. 2. El delito de estafa.

El bien jurídico protegido en el delito de estafa es el patrimonio considerado en su totalidad, lo que comprende en nuestro Derecho todo tipo de cosas -muebles e inmuebles- o derechos<sup>20</sup>. Con esta observación quedan, en principio, solventadas las dificultades que acabamos de apreciar en relación con el delito de hurto y el dinero contable, créditos y otros derechos de contenido patrimonial, que son objeto de protección a través del delito de estafa y a los cuales se suelen dirigir aquellas manipulaciones.

El engaño y el subsiguiente error que caracterizan al delito de estafa<sup>21</sup> han de recaer y originarse sucesiva y exclusivamente en un individuo, mediante el nexo psicológico que se crea entre el engañado y el autor<sup>22</sup>. A partir de aquí es fácil sostener que estos elementos del tipo faltarán casi siempre en las manipulaciones informáticas, particularmente cuando se realizan en la fase de la programación o procesamiento de los datos, pues aquéllas recaen sobre el ordenador sin la intervención de persona alguna a la que realmente se engañe y se induzca a error. En efecto, por lo que se refiere a la manipulación informática como objeto del engaño, es necesario que dicha maniobra sea captada, percibida física o visualmente por una persona, una captación del contenido de los datos manipulados, de forma que como consecuencia de la misma se modifique su representación intelectual sobre la realidad que ha sido falseada<sup>23</sup>. No cabe duda, por consiguiente, que ésta es una exigencia esencial para que el engaño

■ 19 La jurisprudencia ha suscrito la línea argumental de esta tesis en la STS 21 septiembre 1990. V. ya el mismo criterio en la SAP Segovia 27 noviembre 1987, y en la Consulta nº 2/1988 del Fiscal General del Estado.

■ 20 V. por todos, Miguel BAJO FERNANDEZ, *El delito de estafa*, en "Comentarios a la Legislación Penal: La Reforma del Código penal de 1983", t. V, vol. 2º, Madrid 1985, 1160 y ss.

■ 21 Según reza el art. 528 del CP: "Cometen estafas los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de tercero".

■ 22 No se sostiene, por tanto, que haya de tratarse necesariamente de una relación física, como pretende deducir de lo expuesto GUTIERREZ FRANCÉS, *Fraude informático y estafa*, cit., 417 y ss. En su opinión no es preciso un nexo psicológico entre el que engaña y el que realiza el acto de disposición patrimonial, sino que es suficiente con la aptitud del engaño ("engaño bastante", art. 528 CP) para producir dicho error, aunque tal no se produzca (p. 361 y ss.). En mi opinión la aptitud del engaño es incuestionable, pero en el sentido de excluir del tipo aquellos engaños no idóneos, no adecuados, lo que es diferente de la necesidad de que ese engaño -idóneo, apto- haya generado un error en el caso concreto, que conduce al acto final de disposición patrimonial por quien ha sufrido el engaño. El propio texto legal exige que se induzca a realizar un acto de disposición: esa inducción ha de provenir necesariamente de la conducta engañosa que ha dado lugar a un efectivo error, el error 'une' engaño y el acto de disposición.

■ 23 V. SIEBER, *Computerkriminalität und Strafrecht*, cit., 204 y ss.

pueda existir en general, y, lógicamente también, en las manipulaciones informáticas. Así, tal requisito no se dará normalmente en el responsable del departamento de informática de una empresa o banco, al igual que sucede con el operador u otros empleados que tienen un acceso meramente mecánico a los datos y programas, sin alcanzar a ver su contenido ni comprender el sentido exacto de los mismos, ni tener capacidad de ejecución o revisión de las operaciones del ordenador. Estas personas no pueden ser engañadas en tales condiciones.

De todas formas, no siempre está excluida la posibilidad de la percepción del objeto del engaño en el sentido del tipo del art. 528. Ello depende en gran medida del sistema de trabajo y toma de decisiones adoptados por la empresa o institución en la que se utiliza el instrumental informático, en concreto, que la orden incorrecta deba ser ejecutada o supervisada por otro empleado; así como de los métodos de control de cuentas y auditorías y del propio tratamiento y procesamiento de datos. En estos casos sí que podrá concurrir este elemento del tipo. Sin embargo, el reconocimiento de la presencia del engaño incluso cuando han sido adoptados procedimientos regulares de control depende precisamente de cómo se efectúen los mismos. En primer lugar, un control sistemático de todos y cada uno de los procesos en los que son manejados los datos sería materialmente imposible o implicaría unos costes a todas luces desmesurados y desproporcionados con los objetivos de racionalidad en la gestión propuestos. En consecuencia, el control se limita a un muestreo de aquéllos y a los resultados finales de las operaciones contables. Esto significa ya de entrada que las posibilidades de descubrir las eventuales manipulaciones fraudulentas perpetradas por algún empleado se reducen considerablemente, con lo cual no se produce la percepción o captación por parte del auditor de la manipulación de esos datos necesaria para el engaño, y su representación errónea de la situación no estará apoyada en ese engaño, que no se ha llegado a producir<sup>24</sup>. Si por el contrario, descubre la manipulación y con ello el engaño, no se habrá producido el error, pero sí la tentativa de estafa; téngase en cuenta, no obstante, que precisamente por las especiales características operativas del ordenador, el resultado de eliminación de deudas, abono de créditos, etc., suele ser instantáneo, y en consecuencia el descubrimiento de la manipulación será posterior al mismo, lo que no permitirá por si solo la concurrencia de la estafa.

Por su parte, el error ha de recaer sobre *otra persona* y ha de ser originado por el engaño. Este engaño, nos dice el Código penal, ha de ser "bastante para producir error en otro", es decir, que no todo engaño ha de considerarse idóneo para el mismo, sino que ha de ser suficiente, adecuado para producirlo, lo cual

■ 24 LAMPE, *Strafrechtliche Behandlung der sog. Computer-Kriminalität*, cit., 3; SIEBER, *lug. cit.*, 2/12.

ha de medirse de acuerdo con las circunstancias del caso. Se trata aquí de la relación de causalidad entre error y engaño. En conclusión, se puede afirmar que este elemento del tipo del delito de estafa frecuentemente estará ausente en las manipulaciones de datos informatizados, bien por faltar su presupuesto, el engaño, bien porque éste no recae en la formación de la voluntad de una persona, en su representación de la realidad, como requiere el error, sino en las operaciones automatizadas del ordenador<sup>25</sup>. Cuando interfiere en el proceso una tercera persona a causa de la división del trabajo en el seno de la empresa o de los controles periódicos a que se encuentra sometido el personal de la sección de procesamiento de datos, si se ha producido el engaño en los términos expuestos más arriba, sí que podrá generar aquél el error, si esta interferencia ocurre en un momento intermedio entre el engaño y el acto de disposición, lo cual no siempre sucede, pues con frecuencia depende del azar<sup>26</sup>.

Queda por ver otro elemento que ha de concurrir en el delito de estafa, el *acto de disposición patrimonial*. Sólo podrá darse, en primer lugar, si, como veíamos, participa en la gestión de los datos resultantes un empleado responsable antes de que las transferencias dinerarias sean realizadas por el propio ordenador como consecuencia de las órdenes dadas por el autor de las manipulaciones; o, también si es un empleado el que tiene que cargar los abonos ficticios, a la vista de los datos transmitidos por el ordenador una vez tratados informáticamente (*output*). En consecuencia, es necesario que el disponente haya tenido acceso al contenido de los datos informatizados mediante su lectura para que el engaño se haya podido materializar, o lo que es lo mismo, que coincida la condición de disponente y engañado; circunstancia ésta que no siempre se produce, especialmente si, como suele practicarse en las grandes empresas e instituciones bancarias y de ahorro, existe una división funcional del trabajo. Pero, en muchas ocasiones este acto de disposición es realizado directamente por el ordenador (p. ej., abonando una cantidad de dinero en una cuenta preparada a tal fin), de modo que el acto de disposición ya no habrá sido realizado tampoco por una persona.

Por todo lo expuesto, el delito de estafa tampoco reúne las características típicas necesarias para un adecuado castigo de las manipulaciones de datos informatizados, pues o no concurren los elementos del tipo del delito o se origina un engarce desnaturalizado entre los mismos.

■ 25 En este sentido, CORCOY / JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 142; LAMPE, *Strafrechtliche Behandlung der sog. Computer-Kriminalität*, cit., 3; Klaus TIEDEMANN, *Poder económico y delito*, Barcelona 1985, 132.

■ 26 V. Theodor LENCKNER, *Computerkriminalität und Vermögensdelikte*, C.F. Müller, Heidelberg 1981, 27.

### 2.1.3. El delito de apropiación indebida

El delito de apropiación indebida (art. 535 CP) presenta algunos elementos comunes a los delitos de hurto y de estafa<sup>27</sup>, y en esa medida tropieza con las dificultades expuestas. Por otro lado, esta forma de trabajo a través del ordenador exclusivamente, plantearía con frecuencia una seria duda acerca de la presencia de otro elemento típico peculiar del delito de apropiación indebida: haber "recibido en depósito, comisión o administración, o por otro título", etc.; esto no ocurre respecto a programadores, analistas, alimentadores de datos, etc., que no ejercen la custodia o administración del dinero u otros bienes, ni toman decisiones sobre los mismos y son, sin embargo, los que tienen de una u otra forma acceso a los datos informatizados como consecuencia de su actividad profesional<sup>28</sup>.

### 2.1.4. Los delitos de falsificación de documentos.

La obtención de un enriquecimiento patrimonial con perjuicio de tercero mediante el ordenador supone al mismo tiempo una alteración de la realidad contable de la entidad afectada. En este sentido se plantea también la posibilidad de que dicha alteración de la verdad constituya un delito de falsificación de documentos, lo que justifica su estudio, aunque en sentido estricto no constituye un delito patrimonial<sup>29</sup>.

Lo primero que hay que averiguar es si los datos contenidos en un ordenador poseen la naturaleza de un documento. Desde una perspectiva penal, se ha venido considerando tradicionalmente como documento únicamente el escrito, es decir, cuando el pensamiento humano se ha recogido en un soporte material por signos escritos legibles<sup>30</sup>.

Si ahora trasladamos estas observaciones a la manipulación de datos informatizados, nos encontramos, una vez más, con no pocas dificultades. En primer lugar, un programa no encarna en sí mismo un pensamiento o una decla-

■ 27 V. José A. SAINZ-PARDO CASANOVA, *El delito de apropiación indebida*, Barcelona 1978, 51 y ss.

■ 28 Igual sucede en el Derecho alemán: LENCKNER, *Computerkriminalität und Vermögensdelikte*, cit., 28 y ss.; SIEBER, *Computerkriminalität*, cit., 247 y ss, 2/13 y ss.

■ 29 Art. 306 del CP: "El que, con perjuicio de tercero o con ánimo de causárselo, cometiere en documento privado alguna de las falsedades designadas en el art. 302, será castigado con la pena de prisión menor". Según los casos, cabría plantearse también otras modalidades delictivas de falsedad documental, pero la cuestión central queda suficientemente analizada con el delito del art. 306.

■ 30 V. Enrique CASAS BARQUERO, *El delito de falsedad en documento privado*, Barcelona 1984, 226 y ss.; Enrique ORTS BERENGUER, *Derecho Penal, Parte Especial*, 2ª ed. (coord. Tomás VIVES ANTON), Valencia 1988, 227 y ss.

ración de voluntad *concretos de una persona determinada*, sino que, como es sabido, constituye un *instrumento* de trabajo para tratar informáticamente el pensamiento humano. Por tanto, debemos excluirlo ya de entrada de la noción de documento. No sería, por consiguiente, susceptible de encuadrar en este delito la manipulación de los datos mediante la del programa.

Sí que reflejan, por el contrario, un pensamiento humano los datos introducidos en la llamada fase "*input*" en cuanto suministran información de una realidad concreta. Lo mismo puede decirse de la fase del "*output*", o salida de datos, pues no importa que éstos hayan sido tratados o procesados por el ordenador mediante el programa; el pensamiento humano existe con independencia de su manera y origen de formación<sup>31</sup>.

Indudablemente los signos eléctricos recogidos en una cinta o disco magnéticos no constituyen en sí mismos un documento en sentido penal: ni reúnen las características del escrito que sea legible o visualizable, ni de esa idea implícita en el concepto de documento de ser un objeto dotado de cierta materialidad, que no queda satisfecha con la mera existencia de ese disco o cinta.<sup>32</sup> Sin embargo, esa visualización o percepción es posible desde el momento en que se utiliza el ordenador, puesto que aparecen reflejados en la pantalla del mismo de forma escrita. De todos modos, hasta ahí tampoco puede considerarse documento, al no contar todavía con un soporte duradero susceptible de traslación.

En consecuencia, y admitiendo la hipótesis acabada de mencionar, sólo cuando esos datos informáticos manipulados son reproducidos por la impresora del ordenador estaremos ante un documento falso en sentido jurídico-penal. De todas formas, a pesar de esta interpretación funcional, que podría ser discutida, no es suficiente en gran número de casos, en los cuales las operaciones que originan la inexactitud contable que dará lugar a su vez al perjuicio patrimonial se realizan complementamente 'dentro' del mismo ordenador, sin que exista un reflejo externo de las mismas.

Condición del documento en sentido jurídico-penal es también su *atribuibilidad a una persona* por cualquier procedimiento, así como la identificación de su autor<sup>33</sup>. En estos supuestos el que ha manejado el ordenador, ha introdu-

■ 31 De otra opinión, LAMPE, *Die strafrechtliche Behandlung*, cit., 8.

■ 32 A esta conclusión llegan también CORCOY / JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 140. Por otro lado, téngase en cuenta que, por argumentos semejantes a los propuestos en el texto, no existirá nunca delito de falsedad cuando la alteración recaea tan sólo en la banda magnética de una tarjeta de crédito con el fin de ser utilizada en un cajero automático; v. al respecto, más ampliamente, ROMEO CASABONA, *Utilización abusiva de tarjetas de crédito*, cit., 315 y s.

■ 33 V. CASAS BARQUERO, *El delito de falsedad en documento privado*, cit., 253 y ss.

cido los datos o, simplemente, ha dictado las órdenes para el procesamiento de los mismos, asume el resultado obtenido y se convierte de este modo en una declaración de voluntad suya (teoría de la declaración de la voluntad), en su propio pensamiento, pero esa persona no siempre coincide con el manipulador.

## 2.2. Conclusiones y perspectivas de reforma

La comparación de la adecuación de los tipos penales tradicionales de enriquecimiento patrimonial ilícito con las conductas de manipulación de datos informatizados ha querido mostrar la situación insatisfactoria de *lege lata* en que se encuentra el Derecho penal español para incriminar tales conductas debido a la falta de alguno de los elementos del tipo, lo que trae consigo una clara desprotección del bien jurídico del patrimonio. En las hipótesis más optimistas dicha adecuación típica depende de la concurrencia de determinadas circunstancias contingentes, cuando no del azar, pero queda descartada la seguridad de una incriminación con carácter general<sup>34</sup>. Otra conclusión de *lege lata* conduciría a una interpretación forzada de los tipos penales, que muy frecuentemente abocaría en la analogía prohibida; la rigidez que muestran aquéllos impide, además, una interpretación teleológica de los mismos que atendiera al bien jurídico agredido/protegido, o una interpretación evolutiva o progresiva de algunos elementos del tipo, sobre todo los que se refieren a las modalidades de realización de la acción. Por fin, esta situación es muy semejante en derecho comparado, particularmente en aquellos países que presentan afinidades con el nuestro en el ámbito de los delitos patrimoniales o de falsedades documentales, a la vez que una estrecha vinculación con el principio de legalidad.

A la vista del riesgo de lagunas punitivas en nuestro Derecho positivo en relación con la manipulación de datos informatizados, el único camino practicable que nos queda es el de acudir a propuestas de reforma legislativa, a una adaptación de la legislación penal vigente a estas nuevas formas de criminalidad con el fin de despejar las dudas sobre su tipicidad, sin desdeñar tampoco los beneficiosos efectos de prevención general que se derivarían de una adecuada incriminación de estas conductas de enriquecimiento injusto valiéndose del ordenador, ni la necesidad de adoptar medidas preventivas de otra naturaleza no jurídica. Esto debe realizarse introduciendo en el Código penal una nueva figura delictiva, próxima a la de la actual estafa<sup>35</sup>, introduciendo en el nuevo

■ 34 De semejante parecer, para el derecho comparado, SIEBER, *The International Handbook on Computer Crime*, Chichester 1986, 42.

■ 35 V. sin embargo, crítica con este planteamiento, pues lo encuentra demasiado limitado a la vez que estima que el fraude informático tiene cabida en el actual delito de estafa, GUTIERREZ FRANCES, *Fraude informático y estafa*, cit., 619, aunque finalmente lo acepta como función simbólica (621).

tipo los elementos necesarios que suplan los fallos de cobertura de aquélla, en concreto, los elementos del engaño, subsiguiente error y acto de disposición patrimonial: el delito de fraude informático, en cuyo contenido, estructura y engarce con los demás delitos de estafa no puedo ocuparme aquí<sup>36 37</sup>. Para ello habrá que combinar diversos puntos de vista, entre los que desempeñan un factor decisivo de orientación la atención al bien o bienes jurídicos protegidos o merecedores de protección (valores de contenido patrimonial y la fe pública necesaria en el tráfico jurídico), la función normativa de los tipos penales existentes de contenido patrimonial y las formas de agresión (las manipulaciones de datos informatizados), es decir, las acciones ético-socialmente más intolerables frente a las cuales parece conveniente una intervención penal; teniendo también en cuenta el principio de intervención mínima, y el carácter fragmentario del Derecho Penal. Esta afirmación se revela como especialmente adecuada y oportuna en relación con los bienes de contenido patrimonial, para los cuales el ámbito del Derecho privado suele ser normalmente el idóneo para tales fines de protección. En consecuencia, el Derecho penal actuará por medio de la pena cuando junto a determinado desvalor del resultado (lesión o peligro de un bien jurídico) se ha producido un determinado desvalor de la acción (la forma de la conducta agresora) que se estimen merecedores de la pena.

El Proyecto CP de 1992 introduce en el art. 252. 2 la figura de estafa o fraude informático. Frente a las diversas opciones que nos ofrece el derecho comparado, me parece más correcta la del Proyecto, que sustituye de la forma más concisa posible los elementos de la estafa clásica que fracasan en relación con estos comportamientos -como he sugerido más arriba-, si tenemos además

- 36 A ello he dedicado algunas páginas en *Poder Informático y Seguridad Jurídica*, cit., 106 y ss. En concreto, proponía como posible tipo penal el siguiente: "Comete también estafa el que con el fin de obtener un enriquecimiento injusto (o bien: el que con ánimo de lucro) para sí o para tercero en perjuicio de otro\_ altere de cualquier modo el resultado del correcto procesamiento de los datos en conexión con un aparato técnico" (pp. 115 y 117). Como se verá más abajo, el Proyecto CP 1992 introduce un tipo de estafa informática que parte de la misma concepción y estructura que el que propuse entonces, asumiendo que más depurado y sencillo técnicamente que el mío.
- 37 Sobre reformas legislativas de este tenor puede mencionarse, p. ej., la República Federal Alemana, en cuyo Código Penal se han introducido varios delitos que tratan de incriminar de una forma más adecuada los ilícitos de carácter patrimonial cometidos en relación con el uso de ordenadores, a través de la reciente reforma de su Código penal: *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität*, de 15 de mayo de 1986, que entró en vigor el 1<sup>o</sup> de agosto del mismo año. En relación con este delito se ha incluido la 'estafa informática' (§ 263 a). V. más ampliamente sobre esta reforma, Hans A. ENGELHARD, *Computerkriminalität und deren Bekämpfung durch strafrechtliche Reformen*, en "Datenverarbeitung im Recht", 165 y ss. (1985); Theodor LENCKNER/Wolfgang WINKELBAUER, *Strafrechtliche Probleme im modernen Zahlungsverkehr*, en "Wistra", 84 y ss. (1984); Manfred MÖHRENSCHLAGER, *Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG). Entstehungsgeschichte und Überblick*, en "Wistra", 123 y ss. (1986); el mismo, *Das neue Computerstrafrecht*, en "Wistra", 128 y ss. (1986); Ulrich SIEBER, *Informationstechnologie und Strafrechtsreform*, Köln 1985, *passim*; Klaus TIEDEMANN, *Stand und weitere Entwicklung der Bekämpfung der Wirtschaftskriminalität in der Bundesrepublik Deutschland*, en "Juristenzeitung", (1986); Ellen SCHLÜCHTER, *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität*, Heidelberg 1987, 84 y ss.; y ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, cit., 90 y ss. En Francia, por Ley nº 88-19 de 5 de enero de 1988, se han introducido varios delitos en el Código Penal (art. 462); v. al respecto, Michel VIVANT (ed.), *Lamy Droit de L'Informatique*, Paris 1989, 1460 y ss.

en cuenta que es equiparable el desvalor de la acción y del resultado en ambas modalidades de estafa. En cuanto a si es suficiente la descripción de la conducta típica ("realizaren una manipulación informática que interfiera el resultado de un procesamiento o transmisión informática de datos"), es difícil preverlo, pero al menos quedan cubiertas las diversas manipulaciones conocidas en la actualidad, como son las que se refieren a los programas del sistema o de aplicación y a los datos en cualquiera de sus fases del procesamiento informático; aún así, debería reflexionarse sobre la conveniencia de reemplazar la expresión "manipulación informática" por la de "*manipulación*", pues no sé hasta qué punto las realizadas en la consola o en la impresora se pueden calificar de "informáticas", estando por lo demás suficientemente garantizada la conexión informática de los hechos con la referencia al "procesamiento o transmisión informática de datos". De todos modos, estimo más satisfactorio que se sustituya "y así ocasionaren un perjuicio a otro" por "*en perjuicio de otro*" (tal vez mejor entonces situada la expresión a continuación de "con ánimo de lucro"), de forma semejante a la estafa común.

Es acertada también la consideración por parte del Proyecto CP 1992 de llaves a las tarjetas, magnéticas o perforadas (así como los mandos o instrumentos de apertura a distancia, art. 242, párr. 2º), a los efectos del delito de robo con fuerza en las cosas (art. 241 nº 4º), lo que consolida la interpretación que propuse en este sentido en 1987 y permite calificar así por este delito el acceso a los cajeros automáticos con dichas tarjetas para obtener dinero en metálico.

Finalmente, se observan en el Proyecto importantes novedades en relación con los delitos relativos a las falsedades documentales. En primer lugar, incorpora una definición material de documento: "todo papel o soporte material que exprese o incorpore datos, hechos o narraciones de inmediata o potencial relevancia jurídica o eficacia probatoria" (art. 376.1). Por otro lado, el concepto de falsificación de documento se fija más que en los procedimientos en los efectos que comporta para el tráfico jurídico (art. 377). Con ambos preceptos es posible encuadrar un gran número de supuestos de modificaciones de documentos 'informáticos', salvo las dudas que pueden plantearse cuando se trate de alteraciones momentáneas -aunque no en todos los casos-, pero que al ser instrumentales de otro delito, podrán ser castigadas satisfactoriamente por éste.

### 3. *La piratería o copia ilegal de programas*

La importancia que ha ido adquiriendo en nuestro país el tratamiento de la información y de los datos de todo género ha favorecido una paralela e imprescindible creación y perfeccionamiento del soporte lógico (*software*) de los

ordenadores, lo que a su vez ha planteado la necesidad de una adecuada protección jurídica del mismo. Esta necesidad ha permitido comprobar que con frecuencia los instrumentos jurídicos tradicionales de protección de las obras de creación humana de cualquier naturaleza son insuficientes, por la difícil ubicación entre ellas de estos nuevos productos, que comportan con frecuencia una ruptura con los conceptos y estructuras jurídicas hasta ahora utilizados. De ahí que el legislador haya tenido que intervenir en numerosos países -y, como veremos más abajo, incluida España- con el fin de establecer un nuevo marco jurídico que ampare a todas las nuevas manifestaciones del pensamiento y creatividad humanas pero, desde luego, no sólo las vinculadas con las tecnologías de la información.

En derecho comparado<sup>38</sup> y entre los especialistas se ha ido imponiendo el parecer de integrar la protección del soporte lógico dentro de los derechos de autor<sup>39</sup>, que reúne la ventaja de poder atender tanto al aspecto moral (de tanta raigambre en los países latinos) como patrimonial de la propiedad intelectual. El derecho español tradicional antes de la reforma no parecía adecuado de *lege lata* para incluir todas las manifestaciones complejas y variadas que requiere la protección de los programas de ordenador, lo que condicionaba a su vez la intervención del Derecho Penal<sup>40</sup>.

### 3.1. Protección a través de la legislación civil

La Ley de Propiedad Intelectual de 1987<sup>41</sup> supuso un cambio cualitativo en lo que se refiere a la protección de los programas de ordenador y a otras obras de creación y su reconocimiento expreso como objetos de derechos sus-

- 38 En este sentido, contamos con precedentes legislativos en los Estados Unidos, cuya *Copyright* de 1976 fue modificada en 1980 (sec. 101 y 117) con tal finalidad; de igual modo, puede citarse la *Copyright* de 1956 del Reino Unido, modificada en 1985. En la República Federal Alemana la doctrina y la jurisprudencia han venido aceptando la protección de *software* a través de la *Urheberrechtsgesetz*, que contiene cláusulas penales (§ 106), siempre que se trate de programas altamente creativos; esta Ley ha sido modificada en 1985 (24 de junio), con el fin de eliminar dudas acerca de la protección (incluida la penal) de los programas de ordenador. Por fin, la Organización Mundial de la Propiedad Internacional dictó en 1977 unas disposiciones-tipo para la protección del soporte lógico, en esta misma orientación de protección específica de los programas de ordenador a través de los derechos de autor. V. Michael LEHMANN (ed.), *Rechtsschutz und Verwertung von Computerprogrammen*, Köln 1988, *passim*.
- 39 V. ya de este parecer, Eduardo GALAN CORONA, *En torno a la protección jurídica del soporte lógico*, en "Informática e Diritto", 68 y ss. (1983); GONZALEZ RUS, *Aproximación al tratamiento penal de los ilícitos patrimoniales*, cit., 155 y ss.
- 40 Por lo que se refiere a la sustracción de programas de ordenador, en sentido estricto, y su posible represión a través del delito de hurto, v. más ampliamente, ROMEO CASABONA, *Poder informático y seguridad jurídica*, cit., 144 y ss. (147); el mismo, *La protección penal del software en el Derecho español*, en "Actualidad Penal", 1844 y ss. (1988), y en "Cuadernos de Política Criminal", nº 35, 337 y ss. (1988); v. de otro parecer, CORCOY / JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 148 y s. Sobre las dificultades para la punición de la receptación de programas de ordenador y de ficheros informatizados, v. la primera obra citada, 174.
- 41 Ley 22/1987, de 11 de noviembre, modificada por Ley 20/1992, de 7 de julio.

tantivos de autor<sup>42</sup>. Por otro lado, introduce unos mecanismos de protección más ambiciosos, entre los que se incluye una revisión paralela del Código Penal relativa a los delitos contra los derechos de autor.

Como adelantaba más arriba, la Ley de Propiedad Intelectual (LPI) se ha hecho eco de las necesidades de un satisfactorio tráfico jurídico en este ámbito, siguiendo las directrices internacionales apuntadas sobre esta materia. En efecto, sensible con los adelantos tecnológicos, prevé la protección específica de los derechos de autor que afectan a los programas de ordenador (art. 10. 1, i)<sup>43</sup>.

De la definición de objeto de propiedad intelectual y consecuente protección de los derechos de autor podemos entresacar los rasgos que tienen especial relevancia para los programas de ordenador: ha de tratarse de una obra científica, expresada en cualquier medio o soporte, tangible o intangible, y que sea original. En efecto, aunque el soporte del programa es tangible (el disco donde se encuentra registrado) el medio de expresión consiste en unos impulsos (instrucciones) eléctricos(as) intangibles, que son mencionados por la Ley, y por si hubiera dudas sobre su carácter científico -o aunque no lo fuera- incluye en esa relación, que ha de entenderse tan sólo a título ejemplificativo, los "programas de ordenador". Un aspecto que, a mi entender, no ha quedado plenamente delimitado por la Ley es el de cuándo se entiende que es original un programa, dado el extraordinario dinamismo de este sector y las constantes derivaciones y actualizaciones o revisiones a que puede dar lugar (aunque éstas son también objeto de protección por la LPI).

Una vez resuelta afirmativamente la importante cuestión de la protección civil de los programas, hay que ver cuál es el alcance exacto otorgado a la misma, pues de ello dependerá el ámbito de su protección penal, alcance que ha sido establecido en la nueva Ley. Con esta nueva ordenación jurídica de los derechos de autor que afecta a los programas de ordenador y a otras obras de creación de tecnología avanzada, se pretende, según reconoce el Preámbulo de la Ley, que "los derechos y obligaciones de los autores, así como los de los cesionarios de los derechos de explotación puedan quedar delimitados, de acuerdo con las tendencias preponderantes en el actual momento histórico y en beneficio de ambas partes, mediante la aplicación de un *justo equilibrio entre las normas de derecho necesario y el principio de autonomía de la voluntad*". Estas reflexiones y

■ 42 De entre la numerosa e importante bibliografía que ha generado la nueva legislación, mencionamos la colectiva de Rodrigo BERCOVITZ RODRIGUEZ-CANO (coord.), *Comentarios a la Ley de Propiedad Intelectual*, Tecnos, Madrid, 1989.

■ 43 Dice así el art. 10.1 de la nueva Ley: "Son objeto de propiedad intelectual todas las creaciones originales literarias, científicas y artísticas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: i) Los programas de ordenador".

objetivos explican que se les haya otorgado una protección más limitada, la cual ciertamente responde a las especiales características de estas obras, y que se regule en un Título específico, de forma que las demás disposiciones de la Ley serán aplicables subsidiariamente, en defecto de lo prevenido en aquél (art. 95 de la LPI). En efecto, el Título VII del Libro I lleva la rúbrica "De los programas de ordenador", que es el que regula esta materia de forma específica (arts. 95 a 100).

Se asimilan al programa a efectos de tutela la documentación técnica y los manuales de uso de un programa, así como las versiones sucesivas del programa y los programas derivados (art. 96. 2º y 4º)<sup>44</sup>. Las limitaciones o diferencias establecidas para los programas en relación con el régimen general de los derechos de autor son consecuencia de sus propias peculiaridades técnicas. Así, en cuanto a la duración de los derechos de explotación es de cincuenta años desde su publicación o creación (art. 97), mientras que en el régimen general se extiende a toda la vida del autor de la obra y a sesenta años después de su muerte o de la declaración del fallecimiento (art. 26). Otra limitación responde a facilitar el desarrollo y perfeccionamiento del programa y su adaptabilidad a las necesidades del mercado, en cuanto que el autor, salvo pacto en contrario, no puede oponerse a que el cesionario del derecho de explotación realice o autorice la realización de versiones sucesivas de su programa ni de programas derivados del mismo (art. 98), lo que no sería posible en el régimen general, de acuerdo con el cual el procedimiento es el inverso (es el autor el que expresamente debe autorizar en cada caso actuaciones equivalentes en su obra (art. 17). En principio por cesión del derecho de uso se entiende la autorización a utilizar el programa con carácter no exclusivo e intransferible y para satisfacer únicamente las necesidades del usuario, mientras que el cedente conserva la propiedad del programa (art. 99.1 y 2). Sólo es posible la reproducción del programa por parte del usuario para confeccionar la copia de seguridad, pues en otro caso es necesaria la autorización del titular de los derechos de explotación (art. 99.3).

En resumen, puede afirmarse que la protección reconocida a los programas de ordenador se efectúa otorgando prioridad a los intereses de los titulares de los derechos de explotación de los programas en detrimento de los autores materiales de los mismos y de los usuarios.

■ 44 Sus pretensiones de no exclusividad se reflejan en el art. 96. 3, cuando dice: "Los programas de ordenador que formen parte de una patente o un modelo de utilidad gozarán, con independencia de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por la aplicación del régimen jurídico de la propiedad industrial".

### 3.2. Protección en el ámbito penal

La aprobación y promulgación de la Ley de Propiedad Intelectual dio lugar también a la modificación simultánea del Código Penal en relación con la protección penal de los derechos de autor, mediante la introducción de los artículos 534 bis a), 534 bis b), 534 bis c) y 534 ter<sup>45</sup>.

El art. 534 bis a)<sup>46</sup> recoge lo que podríamos considerar tipo básico de este delito, mientras que el art. 534 bis b) contiene unos tipos agravados o cualificados. Por su parte, los arts. 534 bis c) y 534 ter se ocupan de diversos aspectos de la responsabilidad civil derivada del delito, así como la extensión a la vía procesal penal de ciertas medidas cautelares, lo que también habrá de ser objeto de análisis más abajo. Con este (estos) nuevo(s) delito(s) el legislador ha abandonado definitivamente la técnica legislativa de la 'ley penal en blanco', en cuanto que son enunciadas todas las conductas básicas que pueden dar lugar a la infracción penal. De todos modos, para conocer el contenido exacto de las acciones típicas hay que acudir en principio a la LPI -y con mayor razón cuando se refieren a los programas de ordenador-, puesto que se les suele otorgar un significado más restringido que el común y en concreto más limitado todavía para los programas de ordenador frente al alcance que la Ley les reconoce en relación con otros derechos de autor más 'consagrados': se comportan como elementos normativos del tipo.

Veamos brevemente los elementos de este delito centrándonos y acentuando, como es lógico, lo que ofrezca mayor interés para la vulneración de los derechos de autor que recaen sobre un programa de ordenador<sup>47</sup>. La acción con-

- 45 Por Ley Orgánica 6/1987, de 11 de noviembre, por la que se modifica la sección III del Capítulo 4º del Título XIII del Libro II del Código Penal (B.O.E. de 17 de noviembre). V. al respecto, Luis ARROYO ZAPATERO /Nicolas GARCIA RIVAS, *Protección penal de la propiedad intelectual*, en Rodrigo BERCOVITZ RODRIGUEZ-CANO (coord.), *Comentarios a la Ley de Propiedad Intelectual*, cit., 1983 y ss.; Concepción CARMONA SALGADO, la nueva *Ley de propiedad intelectual*, Montecorvo, Madrid 1988; Miguel DIAZ Y GARCIA CONLLEDO, *Los derechos de autor y conexos. Su protección penal: cuestiones generales y naturaleza patrimonial, personal o mixta del bien jurídico protegido*, en "Anuario de Derecho Penal y Ciencias Penales", 803 y ss. (1990); Enrique GIMBERNAT ORDEIG, *Consideraciones sobre los nuevos delitos contra la propiedad intelectual*, en "Poder Judicial", nº especial IX, 351 y ss. (1989); Gonzalo QUINTERO OLIVARES /José M. GOMEZ BENITEZ, *Protección penal de los derechos de autor y conexos*, Civitas, Madrid 1988; Francisco SOTO NIETO, *Delitos contra los derechos de los titulares de la propiedad intelectual*, en "Poder Judicial", nº especial IX, 369 y ss. (1989).
- 46 Dice lo siguiente "Será castigado con la pena de multa de 100.000 a 2.000.000 pesetas quien intencionadamente reproducere, plagiar, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística o científica o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondrá a quien intencionadamente importare, exportare o almacenare ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización".
- 47 V. más ampliamente, sobre la importante polémica relativa a la naturaleza del bien jurídico protegido, DIAZ Y GARCIA CONLLEDO, *Los derechos de autor y conexos*, cit., 817 y ss., cuya tesis mixta suscribo; y sobre los elementos del delito, ROMEO CASABONA, *Poder informático y seguridad jurídica*, cit., 156 y ss.; el mismo, *La protección penal del software en el Derecho español*, cit., 1836 y ss., y 325 y ss., respectivamente.

siste en 'reproducir', 'plagiar', 'distribuir', 'comunicar públicamente' (total o parcialmente) o 'transformar' una obra literaria, artística o científica, etc., o su 'importación', 'exportación' o 'almacenamiento'. Penando el plagio se quieren proteger los derechos morales del autor sobre su obra, mientras que las demás conductas se refieren a los derechos de explotación de aquélla. De la LPI podemos deducir en la mayor parte de los casos qué debemos entender por cada una de estas conductas. Hay que ver, en primer lugar, cómo afecta el plagio<sup>48</sup> a los programas de ordenador. No constituye plagio la realización de versiones sucesivas de un programa de ordenador ni de programas derivados del mismo por parte del cesionario titular de los derechos de explotación, salvo que hubiera mediado pacto en contrario con el autor (art. 98 de la LPI), pues se pretende con ello facilitar su perfeccionamiento o adaptación a la función específica que se le quiera dar. Como podemos comprobar, el derecho moral del autor de un programa está muy limitado legalmente y si además tenemos en cuenta que las versiones sucesivas y los programas derivados son también objeto de protección expresa por la LPI (art. 96. 4), el requisito de originalidad queda muy reducido en esta clase de obras.

En cuanto a la reproducción, se entiende la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella (art. 18 de la LPI). Sin embargo, en lo relativo al programa de ordenador el concepto de reproducción es más limitado, pues no se considera como tal la introducción del programa en memoria interna a los solos efectos de su utilización por el usuario (art. 99. 3 de la LPI); ni tampoco la copia de seguridad (art. 99. 2 de la LPI). En los demás casos, la reproducción del programa, incluso para uso personal, exigirá la autorización del titular del derecho de explotación. Limitaciones al ejercicio exclusivo de este derecho de explotación justificada, una vez más, por las características técnicas de funcionamiento de estas obras.

La distribución y la comunicación pública no ofrece especiales particularidades en relación con los programas, salvo recordar que es posible distribuirlos y comunicarlos<sup>49</sup> a otros usuarios por medio del mismo ordenador a otro ordenador, si están conectados entre sí (a través de un *modem*), pues, como

■ 48 Sobre el significado de plagio a los efectos del tipo y su relación y diferenciación de usurpación de la condición de autor (art. 534 bis b, párr 1º c), que constituye una forma agravada del plagio (en este sentido, ARROYO ZAPATERO / GARCIA RIVAS, *Protección penal de la propiedad intelectual*, cit., 1994 y s. y 2002), véanse las referencias de la nota anterior.

■ 49 El requisito de publicidad en la comunicación no está excluido por este medio sí, por ejemplo, el ordenador de destino es de acceso común a una pluralidad no cerrada de usuarios. Véase, al respecto, la LPI art. 20. 2. h), que considera que son actos de comunicación pública "el acceso público a bases de datos de ordenador por medio de telecomunicación, cuando éstas incorporen o constituyan obras protegidas". Además de que este artículo no constituye una descripción cerrada de supuestos de comunicación pública, pienso que no hay inconveniente en asimilar un programa de ordenador a los datos contenidos en una base de ellos.

sabemos el programa tiene como destino natural un ordenador. La utilización de este mismo procedimiento rebasando las fronteras nacionales (lo que sabemos que es relativamente fácil) dará lugar a las conductas típicas de importar o exportar a que se refiere el 2º párr. del art. 534 bis a. Por transformación de una obra hay que entender, de acuerdo con la LPI, su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente (art. 21. 1). Sin embargo, para los programas no constituye transformación la adaptación de un programa realizada por el usuario para la utilización exclusiva por el mismo (art. 99. 4 de la LPI)<sup>50</sup>, ni la ya indicada realización o autorización de realización de versiones sucesivas del programa ni de programas derivados del mismo por parte del cesionario titular de los derechos de explotación.

En el artículo 534 bis b) se recogen varios tipos agravados, que responden sobre todo a una más estricta protección de los derechos morales, aunque también se refuerce en ciertos casos (cuando medie el ánimo de lucro) la protección penal de los derechos de explotación<sup>51</sup>. Para el examen de estos tipos agravados conviene separar otra vez los que se refieren a atentados contra los derechos morales de los que conculcan los derechos de explotación. En cuanto a las infracciones contra los derechos morales del autor, a ellas se refieren las letras b, c y d del art. 534 bis b. Es de reseñar que la vulneración de estos derechos hay que ponerla en conexión con las conductas prevenidas en el artículo anterior (art. 534 bis a), de modo que por lo general se habrán infringido ya los derechos de explotación mencionados en el mismo, pero que darán por resultado una ulterior vulneración de los derechos morales contemplados en el art. 534 bis b. Infringir el derecho de divulgación del autor significa no respetar la decisión del autor sobre si la obra ha de ser divulgada y en qué forma (art. 14. 1º de la LPI), así como si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente (art. 14. 2º de la LPI). En relación con el programa de ordenador hay que tener en cuenta lo dicho en cada una de estas conductas del tipo básico. Por lo que se refiere a usurpar la condición de autor sobre una obra o parte de ella (o el nombre de un artista en una interpretación o ejecución), ya

- 50 Por esta razón tampoco le afecta lo dispuesto en el art. 11. 5º de la LPI: "Sin perjuicio de los derechos de autor sobre la obra original, también son objeto de propiedad intelectual: 5º Cualesquiera transformaciones de una obra literaria, artística o científica".
- 51 Dice así el art. 534 bis b: "1. Será castigado con la pena de arresto mayor y multa de 175.000 a 5.000.000 pesetas quien realizare cualquiera de las conductas tipificadas en el artículo anterior, concurriendo alguna de las siguientes circunstancias: a) Obrar con ánimo de lucro. b) Infringir el derecho de divulgación del autor. c) Usurpar la condición de autor sobre una obra o parte de ella o el nombre de un artista en una interpretación o ejecución. d) Modificar sustancialmente la integridad de la obra sin autorización del autor. 2. Se impondrá la pena de prisión menor, multa de 175.000 a 10.000.000 pesetas e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando, además de obrar con ánimo de lucro concurra alguna de las siguientes circunstancias: a) Que la cantidad o el valor de las copias ilícitas posean especial trascendencia económica. b) Que el daño causado revista especial gravedad. En tales supuestos el Juez podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado".

me he ocupado más arriba, al referirme al plagio. Esta conducta no ofrece ninguna particularidad destacable cuando afecta a un programa de ordenador. Por último, al modificar sustancialmente la integridad de la obra se infringe el derecho exclusivo del autor de exigir el respeto de su integridad e impedir cualquier deformación, modificación, alteración, o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación (art. 14. 4º de la LPI); tal facultad de modificación corresponde exclusivamente al autor (art. 14. 5º de la LPI). Ya hemos visto que, salvo pacto en contrario, es muy limitado el poder de control sobre dicha integridad que se reconoce al autor de un programa.

Por otro lado, el CP configura unas infracciones contra los derechos de explotación del autor. Para que existan estos tipos agravados es preciso que se actúe con ánimo de lucro, con independencia de que se haya producido un efectivo perjuicio económico a los titulares o cesionarios de los derechos de propiedad intelectual. Este elemento subjetivo de lo injusto constituye el único punto de conexión de estos delitos con los delitos contra el patrimonio (Título XIII), pues en las demás conductas no es precisa la presencia de este ánimo ni la causación de un perjuicio económico.

Si, además del ánimo de lucro, la cantidad o el valor de las copias ilícitas poseen especial trascendencia económica o el daño causado reviste especial gravedad, nos encontraremos ante un tipo 'superagravado', que comporta, además de una elevación de las penas de privación de libertad y pecuniaria, la de inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido y la facultad del cierre temporal o definitivo de la industria o establecimiento del condenado, que actúa como medida de seguridad más que como pena accesoria. Este fenómeno es el que con más frecuencia se dará en la infracción de los derechos de autor de programas de ordenador<sup>52</sup>, pues la llamada piratería de programas (al igual que la de cassettes y películas de vídeos) persigue por lo general la obtención de un beneficio económico a costa de sus creadores o de los titulares de los derechos de explotación, a diferencia de otras obras, en las que es posible pretender conseguir una emulación o reputación intelectual.

Especial interés reviste la responsabilidad civil prevista en los artículos 534 bis c y 534 ter<sup>53</sup>. El primero de ellos contempla una especie de reparación

■ 52 V. al respecto ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, cit., 141 y ss.

■ 53 Dicen así: art. 534 bis c: "En el supuesto de sentencia condenatoria el Juez podrá decretar la publicación de ésta, a costa del infractor, en un periódico oficial". Art. 534 ter: "La extensión de la responsabilidad civil derivada de los delitos tipificados en los artículos 534 bis a y 534 bis b, se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios". V. José JIMENEZ VILLAREJO, *La responsabilidad civil dimanante de las infracciones de la propiedad intelectual y las vías judiciales para su exigencia*, en "Poder Judicial", nº especial IX, 359 y ss. (1989).

moral para el autor, sin perjuicio de otras reparaciones o indemnizaciones por el daño moral sufrido. El segundo remite directamente a la LPI (arts. 123 a 128) para la indemnización de los daños y perjuicios, sin que sea necesario acudir para los supuestos más específicos a la vía civil paralela o posterior (haciendo, por ejemplo, reserva de las acciones civiles en el proceso penal), como es el cese de la actividad ilícita (art. 124 de la LPI), incluso en lo concerniente a la solicitud con carácter previo de las medidas cautelares de protección urgente<sup>54</sup>, como prevé de forma expresa la referida Ley<sup>55</sup>.

El Proyecto de 1992 viene a resolver las dudas que pudiera plantear en la actualidad la protección penal de las topografías de los productos semiconductores<sup>56</sup>, dada su naturaleza aparentemente mixta de creación intelectual y de producción industrial, decantándose por esta última vía de forma expresa (art. 281. 3).

#### 4. Espionaje informático

Consiste en la obtención sin autorización de datos almacenados en un fichero informatizado. Al igual que el fraude informático, lo que ahora llamamos espionaje informático tiene unos efectos económicos de primera magnitud<sup>57</sup>, favorecidos por la todavía notable desprotección material y logística de las bases de datos informatizados, a pesar de la existencia de restricciones de acceso (p. ej., *password*) y de lectura de los datos (encriptamiento o codificación de los datos); ello se explica por el hecho de hallarse la información gracias a este sistema concentrada en un espacio muy reducido y es susceptible de copia por esta misma razón en un soporte pequeño y en un lapso de tiempo insignificante. En el ámbito comercial afecta a las contabilidades de las empresas, balances, cartera de clientes, mientras que en el puramente tecnológico a datos de investigación y desarrollo de tecnología; igualmente al *know how*, o conocimiento de procedimientos económicos y tecnológicos de carácter, en principio, reservado<sup>58</sup>, de tanta importancia en el tráfico económico actual de las empresas. Evidentemente, este tipo de espionaje adquiere particular relieve con otras fina-

- 54 Art. 126 y 127; éste último señala el procedimiento a seguir por la vía civil, con algunas especialidades.
- 55 Art. 128: 'Las medidas cautelares previstas en el artículo 126 podrán ser acordadas en las causas criminales que se sigan por infracción de los derechos reconocidos en esta Ley. En su tramitación se observarán las reglas del artículo 127, en lo que fuera pertinente. Las mencionadas medidas no impedirán la adopción de cualesquiera otras establecidas en la legislación procesal penal'.
- 56 V. Ley 11/1988, de 3 de mayo, de Protección jurídica de las topografías de los productos semiconductores.
- 57 Sobre la información como valor económico digno de protección penal, v. Jean-Pierre CHAMOUX (ed.), *L'appropriation de l'information*, Paris 1985, 17 y ss.; ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, cit., 168 y s.
- 58 V. al respecto, TIEDEMANN, *Poder económico y delito*, cit., 111 y ss.

lidades, como es el realizado en los secretos de los Estados o de las organizaciones supranacionales de cooperación militar, particularmente en lo relativo a la defensa y la seguridad. Anecdóticas son por el momento, aunque no dejan de ser significativas del peligro real existente y de la vulnerabilidad de los ficheros informáticos, las incursiones de los llamados *hackers*, jóvenes que acceden a bases de datos de lo más variadas (bancos, grandes comercios, hospitales, centros de seguridad de los gobiernos, etc.), con el fin de vencer el reto que supone para ellos el acceso a las mismas valiéndose de un microordenador y de la conexión a través de la línea telefónica.

#### *4.1. Protección penal*

Desde el punto de vista jurídico son más complejos, si cabe, los problemas que encierra el tratamiento penal del espionaje informático en comparación con el fraude informático, tanto desde la vertiente penal como del Derecho privado. Necesariamente, en este trabajo sólo podemos aspirar a una inicial aproximación a su entramado jurídico-penal.

La protección penal de los datos contenidos en un fichero informático, frente al acceso no autorizado o la copia de los mismos, plantea el problema de la adecuación de la conducta con algunos tipos delictivos que protegen el patrimonio o los secretos. El delito de hurto no sería aplicable al caso por las mismas razones que indiqué en relación con el fraude informático: no se trata de cosa mueble, la acción recae sobre elementos intangibles o incorporales no susceptibles de apoderamiento en el sentido del art. 514 del CP; además, el propietario no es privado en realidad del fichero informático, el cual permanece en su poder, sino que es únicamente copiado.

Su reconducción dentro la protección de la propiedad intelectual encuentra la dificultad de su consideración como obra científica, de creación y original, así como que estos ficheros mantienen su virtualidad mientras son secretos, lo que no sucede con los derechos de autor; aparte de que por lo general no se incurre en una reproducción -pública- del fichero, pues éste es utilizado por el propio autor (tal vez incluso sin necesidad de copiar el fichero); si lo vende a un tercero (a una empresa), podría entenderse realizada ya su reproducción o su distribución en el sentido de las conductas prohibidas por el art. 534 bis a del CP. Por otro lado, la LPI de 1987 considera un acto de comunicación pública el acceso público a bases de datos de ordenador por medio de telecomunicación, cuando éstas incorporen o constituyan obras protegidas por dicha Ley (art. 20.2 h). En consecuencia, es una de las conductas integradas en los derechos de explotación, penalmente protegidos por el art. 534 bis a. Sin embargo,

esta interpretación no proporciona un apoyo jurídico suficiente como para poder deducir que la LPI considere las bases de datos siempre incluidas en cuanto tales dentro de su ámbito de protección.

Si, a pesar de todo, los datos no poseen la calificación de reservados, y únicamente en esta eventualidad, cabe también plantearse su castigo como competencia ilícita, a tenor de lo previsto por la Ley de Propiedad Industrial (arts. 131 y 132) en conexión con el art. 534 del Código penal, pero siempre que esa base de datos posea un contenido susceptible de protección industrial, lo que no será tan frecuente, si tenemos presente el catálogo de conductas que incluye la referida Ley.

Por último, tampoco parece viable una incriminación satisfactoria dentro de los delitos de descubrimiento y revelación de secretos (en concreto, los supuestos del art. 497, pues exige el apoderamiento de papeles o cartas de otro, que no es nuestro caso ni en cuanto a la conducta ni en cuanto a los objetos), al igual que sucede con la protección de los datos que afectan a la intimidad de las personas, con el inconveniente añadido aquí que este espionaje informático industrial persigue el ánimo de lucro, de ninguna manera cubierto por estos delitos<sup>59</sup>. Sólo los tipos de los artículos 498 y 499<sup>60</sup> ofrecen la posibilidad de cierta cobertura, pero en cualquier caso limitada, puesto que únicamente alcanza a empleados de la empresa y no, por consiguiente, cuando se realiza por personas ajenas a ella (p. ej., por conducción telefónica), ha de tratarse de descubrir datos secretos y, en el supuesto del artículo 499, han de ser secretos industriales, lo que no impide entenderlos en sentido amplio, incluyendo también los de carácter comercial<sup>61</sup>. Si la obtención de los datos se logra por una persona ajena interfiriendo en la comunicación entre dos ordenadores (o un ordenador y un terminal), como ésta se efectúa valiéndose de la línea telefónica, entraría en juego el delito del art. 497 bis (interceptación de comunicaciones telefónicas), haciendo notar, no obstante, que el componente patrimonial del hecho no quedaría suficientemente reflejado en su represión.

#### 4.2. *Perspectivas de reforma*

Las reflexiones acabadas de exponer abundan en la idea de la clara des-

- 59 Y ello a pesar de lo que dispone el art. 499, como veremos a continuación.
- 60 Art. 499: "El encargado, empleado u obrero de una fábrica u otro establecimiento industrial que en perjuicio del dueño descubriere los secretos de su industria será castigado con las penas de arresto mayor y multa de 100.000 a 1.000.000 pesetas". Si los hechos son cometidos por funcionario público, no existirían especiales dificultades de incriminación a través de los arts. 367 y 368 del CP conforme a su redacción por LO 9/1991, de 22 marzo, pues no exigen una modalidad comisiva concreta (así, el primero comienza: "El funcionario público o autoridad que revelare los secretos o cualquier información de que tenga conocimiento por razón de su oficio o cargo..."). La misma opinión en ambos casos sustentan CORCOY / JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 145 y ss.
- 61 V. Miguel BAJO FERNANDEZ, *Derecho Penal económico*, Madrid 1978, 295 y ss.

protección existente en nuestro ordenamiento jurídico frente al espionaje informático, aunque quede parcialmente cubierto por el delito de revelación de secretos industriales y excepcionalmente por el de infracción de los derechos de autor; y no sólo frente a estas conductas abusivas, sino también frente al mero acceso a los datos. De ahí la conclusión de la necesidad de promover una adecuada y más amplia protección penal (pero no sólo penal).

Salvo las observaciones ya apuntadas, nada se dice en la LPI sobre la naturaleza de los datos de un fichero informático y su posible objeto de propiedad intelectual. Sin embargo, dado que dicha Ley no pretende ser exhaustiva en cuanto a la enumeración de creaciones originales literarias, científicas y artísticas susceptibles de propiedad intelectual, cabría también la inclusión de los datos, siempre que puedan ser calificados de 'creación literaria, científica o artística', lo cual queda en entredicho. De todas formas, aunque aceptáramos su naturaleza de científicos, no parece que sea ésta la vía más adecuada para todos los supuestos, pues la nota más característica es la del carácter reservado de esos datos, y el espionaje informático afectará entonces a la capacidad competitiva de la empresa. Es, por tanto, en atención a estas dos peculiaridades donde debe centrarse la reforma penal o la de la legislación específica con el fin de conseguir que actúe en ambas de forma complementaria (creación intelectual y secreto). No debe olvidarse tampoco, en cualquier caso, la protección frente a los accesos no autorizados a bases de datos, siempre que fueran intencionados, o siendo accidentales, el intruso se mantuviera voluntariamente en ellos<sup>62</sup>. No obstante, hay que tomar la precaución de evitar una desmesurada protección de la información por sí misma, lo que podría favorecer un monopolio de la protección del secreto industrial sobre la información<sup>63</sup>.

Dentro del espionaje industrial el Proyecto CP 1992 da cabida al espionaje informático (art. 284. 1)<sup>64</sup>, para cuya descripción típica completa se remite al art. 198, ya comentado. Este delito refuerza la impresión de que el art. 198 debe ser completado en los términos que he propuesto más arriba, pues también

■ 62 El espionaje de datos ha sido elevado a delito en la República Federal Alemana, tras la reciente reforma citada de 1986, en su párrafo 202 a. V. SIEBER, *Informationstechnologie und Strafrechtsreform*, cit., 49 y ss., en favor de la introducción de un precepto de este tenor (cuando el Proyecto de reforma no preveía su inclusión). Sobre este párrafo, v. SCHLÜCHTER, *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität*, cit., 56 y ss.; TIEDEMANN, *Stand und weitere Entwicklung der Bekämpfung der Wirtschaftskriminalität in der Bundesrepublik Deutschland*, cit., 865 y ss. También la reforma del CP francés de 5 de enero de 1988, art. 462. 2.

■ 63 V. en este sentido, SIEBER, *The International Handbook on Computer Crime*, cit., 59.

■ 64 Art. 284.1: "El que para descubrir o revelar un secreto de empresa evaluable económicamente y que comporte ventajas competitivas, se apoderare de documento, soporte informático u otros objetos, o empleare alguno de los medios o instrumentos señalados en el artículo 198, será castigado con la pena de prisión de seis meses a dos años y multa de doce a veinticuatro meses. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos".

es posible acceder a un secreto empresarial sin necesidad de apoderarse de dato alguno ni del soporte informático correspondiente, como es la simple visualización de los datos en pantalla reteniéndolos memorísticamente o copiándolos a mano. Con la inclusión en el art. 198. 2 de la expresión "utilizar" creo que se abarca de forma suficiente este supuesto, que puede originar perjuicios económicos de especial magnitud. Con independencia de esta observación, queda por ver qué se ha de entender por "secreto de empresa", siendo de suponer que por tal habrá que abarcar lo que la propia empresa quiera mantener reservado mediante actos concluyentes.

### 5. Sabotaje informático

Como hemos visto, el 'sabotaje informático' consiste en la destrucción o inutilización del soporte lógico, esto es, de datos y/o programas contenidos en un ordenador (en sus bandas magnéticas)<sup>65</sup>. Indudablemente, es posible asimismo la destrucción o inutilización del soporte físico del sistema informático (*hardware*), agresiones que no ofrecen, en principio, mayores particularidades<sup>66</sup>. Existen diversos procedimientos, la mayoría de ellos, al menos los más eficaces y difíciles de detectar, se sirve de la propia tecnología del ordenador, que conducen al borrado total o parcial de los datos o del programa, a su inoperatividad o a la imposibilidad de acceso a los mismos (procedimientos conocidos como 'caballo de troya', 'bombas lógicas', 'virus informático', etc.). Dentro de este conjunto de conductas hay que incluir la introducción de datos nuevos erróneos o la alteración de los ya procesados (siempre que no sea con ánimo de enriquecimiento, lo que nos trasladaría al fraude informático, o de alterar la llamada identidad informática, que nos movería dentro de los ataques a la intimidad individual), pues su finalidad es la misma, la de que el fichero manipulado pierda la función a la que estaba destinado.

La perpetración de estos actos de sabotaje suele ir dirigida a la causación de un perjuicio patrimonial en el titular o usuario del ordenador (empresas, entidades bancarias o de ahorro), perjuicio que suele alcanzar cifras muy elevadas, lo cual se comprende fácilmente, pues se le priva de todo su sistema de gestión (contabilidad, administración, cartera de clientes) o, incluso, de planificación y organización del trabajo, así como la actividad empresarial misma (diseños industriales, las fuentes de las agencias dedicadas a proveer información a su

■ 65 V. más ampliamente Mirentxu CORCOY BIDASOLO, *Protección penal del sabotaje informático. Especial consideración de los delitos de daños*, en "La Ley", nº 2.400, 1 y ss. (1990); Carlos M. ROMEO CASABONA, *Los delitos de daños en el ámbito informático*, en "Cuadernos de Política Criminal", 91 y ss. (1991).

■ 66 V. al respecto, nota anterior y GONZALEZ RUS, *Aproximación al tratamiento penal*, cit., 126 y ss.; SIEBER, *The International Handbook on Computer Crime*, cit., 15 y s.

clientes, etc.). Junto a estos daños no son desdeñables tampoco los que se pueden irrogar con finalidad política contra la seguridad y defensa de los Estados (p. ej., sobre armamento y organización operativa de las fuerzas armadas, ficheros de la policía).

### 5.1. *Incrimación de estas conductas*

El Código penal español, del mismo modo que los Códigos de otros países, conoce el delito de daños (art. 557 y ss.), que parece el más adecuado para reconducir penalmente los hechos de los que nos ocupamos ahora, dado su evidente paralelismo. La principal dificultad con que nos encontramos para la incriminación de estos actos de sabotaje radica en que el daño se efectúa en el soporte lógico (elemento no físico, incorporeal) del sistema informático: ésta es la cualidad de los datos y programas, que son meros impulsos eléctricos plasmados normalmente en un soporte material (la banda o disco magnéticos). Por otra parte, según entiende la doctrina española, el objeto material sobre el que ha de recaer el delito de daños habrá de ser una "cosa ajena o propia, mueble o inmueble, material y económicamente valorable, susceptible de deterioro o destrucción y de ejercicio de la propiedad"<sup>67</sup>. Todas estas condiciones las reúnen los datos o programas de un ordenador (no cabe duda, por ejemplo, del valor económico que éstos poseen), salvo el de ser una cosa material. En otros países se fijan en el contenido patrimonial de lo dañado más que en la naturaleza corporal o incorporal de la cosa, pudiendo de este modo castigar estos hechos como delito de daños<sup>68</sup>. La materialidad de la cosa, que tiene sentido en los delitos de apoderamiento, puesto que requieren la aprehensión de la misma, no tiene base en estos delitos<sup>69</sup>, si partimos de una interpretación evolutiva de los mismos, atendiendo al bien jurídico protegido; lo relevante es que se dañe algo susceptible de propiedad y valuable económicamente. Por consiguiente, los delitos de daños del CP vigente integran sin especiales dificultades estas conductas<sup>70</sup>.

Aceptado lo anterior, importa dilucidar si el daño en la cosa (el fichero de datos) ha de afectar al valor de su sustancia (*Substanzwerttheorie*) o al del uso

- 67 V. por todos, Agustín JORGE BARREIRO, *El delito de daños en el Código penal español*, en "Anuario de Derecho Penal y Ciencias Penales", 513 (1983).
- 68 V. LENCKNER, *Computerkriminalität und Vermögensdelikte*, cit., 19.
- 69 En este sentido, GONZALEZ RUS, *Aproximación al tratamiento penal*, cit., 139 y s.
- 70 V. CORCOY BIDASOLO, *Protección penal del sabotaje informático. Especial consideración de los delitos de daños*, cit., 7. La sentencia de la AP de castelón, 2 mayo 1989, ha mantenido este criterio, pues castigó por un delito de daños (art. 563 en relación con el art. 560. 1) porque unos disquetes fueron estropeados por unos jóvenes al accionar un extintor (parece que intencionadamente) y contenían un trabajo de investigación realizado por la víctima en los dos últimos años.

a que originariamente estaba destinada (*Gebrauchstwerttheorie*)<sup>71</sup>. Sólo si admitimos esta segunda interpretación<sup>72</sup> podremos acoger dentro del delito de daños no sólo la destrucción sino también la inutilización del soporte lógico del ordenador, pues éstas afectan a su operatividad (a la utilización normal del programa o de los datos) sin que se destruya ni altere al mismo tiempo (al menos necesariamente) el disco o banda magnética donde se encuentra recogido, ni mucho menos el funcionamiento del ordenador.

La importancia de esta distinción se explica porque el Código penal castiga el delito de daños con pena de mayor o menor gravedad atendiendo, entre otros criterios, al valor del daño causado. En relación con este punto se plantea la siguiente cuestión: si la víctima poseía copias actualizadas (idénticas) de seguridad de los datos o del programa, en su caso, y la destrucción o inutilización no alcanza a éstas, la pregunta es si podrá entenderse consumado el delito. En mi opinión sólo se ha producido el desvalor de la acción, y el hecho será punible en grado de tentativa, puesto que esas copias son utilizables de forma inmediata. Por el contrario, si aquéllas fueron destruidas junto con los originales (único medio de que el autor consiga realmente sus propósitos) o no estaban actualizadas, o no existían o los contenidos se habían transcrito tan sólo en papel, el delito se habrá consumado.

## 5.2. Propuestas de reforma

A pesar de las conclusiones de punibilidad de los actos de sabotaje a través de los delitos de daños a que hemos llegado, no debe descartarse una intervención del legislador para una mejor cobertura penal de estas conductas, en cuyo caso me inclino por la vía de completar los tipos existentes allí donde resulte necesario, a la vista de los puntos que han sido objeto de duda o discusión, sin necesidad de crear ningún tipo autónomo o específico<sup>73</sup>, incluso aunque sólo fuera para lograr unas penas más adecuadas al desvalor de estos hechos<sup>74,75</sup>. Si llegara el caso, debería procederse con gran cautela, limitando

■ 71 V. Agustín JORGE BARREIRO, *El delito de daños en el Código penal español*, cit., 513.

■ 72 Incluso GONZALEZ RUS, lug. cit., 141 y s., estima que la información del fichero que resulta destruida 'es' la sustancia misma del objeto dañado.

■ 73 Que, según se ha visto, se centran en las modalidades de comisión (la destrucción, deterioro o inutilización, entendiendo dentro de ésta en nuestro caso también la alteración de los datos o imposibilitar su acceso o utilización efectiva) y en el objeto sobre el que ha de recaer la acción (habría que incluir los bienes incorpóreos susceptibles de daños en general o, de modo específico, los datos).

■ 74 Coinciden con estos criterios de *lege lata* y de *lege ferenda*, CORCOY / JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 149 y s. y 153; CORCOY BIDASOLO, *Protección penal del sabotaje informático. Especial consideración de los delitos de daños*, cit., 7.

■ 75 Por ejemplo, el legislador alemán ha estimado oportuno introducir el delito de 'sabotaje informático' (§§ 303 a, 303 b), en la mencionada *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität*. V. también el CP francés, art. 462. 2 (segundo párr.), 3 y 4, e información en VIVANT (ed.), *Lamy Droit de L'Informatique*, cit., 1498 y ss.

la incriminación a las conductas intencionales, con el fin de evitar un castigo no deseable de conductas negligentes o de errores o fallos técnicos<sup>76</sup>.

#### 6. Agresiones en el soporte material informático

El único comportamiento agresivo en el soporte material informático (aparte de los daños físicos) que presenta ciertas novedades -y ello hasta cierto punto- vinculadas a estas tecnologías se reduce en la práctica al hurto de uso del tiempo del ordenador<sup>77</sup>, es decir la utilización sin autorización de un ordenador por un tercero durante un tiempo determinado sin que implique la traslación física del aparato. La importancia económica de estas incursiones es menor, pero tampoco desdeñable. Por supuesto, su interés radica no en el consumo energético, sino en valerse gratuitamente y sin autorización de una alta tecnología que, en sus prestaciones más sofisticadas, es todavía muy costosa<sup>78</sup>.

No ofrece dificultad afirmar que esta modalidad de agresión 'informática' no es susceptible de incriminación en nuestro Derecho vigente, pues el hurto de uso con ánimo de lucro no constituye un ilícito penal con carácter general, con la sola excepción del delito utilización ilegítima de vehículos de motor ajenos (llamado impropriamente también hurto de uso), del artículo 516 bis del CP<sup>79</sup>, ni habría ninguna otra figura delictiva de enriquecimiento del CP español (como las defraudaciones de fluido eléctrico y otras análogas) donde integrar estos hechos.

Finalmente, no parece oportuno, desde una perspectiva político-criminal, la incriminación de estos hechos en el momento actual, por su probable escasa incidencia en nuestro país, y porque el Derecho Penal, como ya he señalado en más de una ocasión, sólo debe intervenir cuando fracasen otros sectores del ordenamiento jurídico<sup>80</sup>.

■ 76 De este parecer, SIEBER, *The International Handbook on Computer Crime*, cit., 81.

■ 77 Es cierto que junto a la utilización indebida del ordenador puede confluír la de programas y datos, lo que nos llevaría a lo expuesto más arriba en relación con estas conductas.

■ 78 V. casuística en Louis ROHNER, *Computerkriminalität. Strafrechtliche Probleme bei 'Zeitdiebstahl' und Manipulationen*, Zürich 1976, 11 y ss.

■ 79 V. en este sentido, GONZALEZ RUS, *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, cit., 121; Rodrigo Fabio SUAREZ MONTES, *Robo y hurto de uso de vehículos de motor*, en "Revista General de Legislación y Jurisprudencia", 5 (1970).

■ 80 De esta opinión, LENCKNER, *Computerkriminalität und Vermögensdelikte*, cit., 21; SIEBER *Informationstechnologie und Strafrechtsreform*, cit., 59. En sentido contrario, ROHNER, *Computerkriminalität*, cit., 29; mantiene una postura alternativa de *lege ferenda*, CORCOY / JOSHI, *Delitos contra el patrimonio cometidos por medios informáticos*, cit., 154; Referencias de derecho comparado favorables a su incriminación en ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, Fundesco, cit., 180.

