El fraude informático. ¿Un riesgo asegurable?

JUANA MARÍA DOMAICA MAROTO

Facultad de Derecho. Universidad de Comillas. ICADE.
Beca Programa «Riesgo y Seguro» de
Fundación MAPFRE Estudios

Se puede afirmar que si el Código Penal es una de las normas que refleja el orden valorativo de la sociedad, la sensibilidad dominante en el ámbito empresarial español reclama la configuración de unos nuevos tipos penales presididos por el principio de defensa de uno de los activos, hoy, más valiosos en cualquier entidad: el procesamiento automático de su información.

La delincuencia informática, ¿la gran ignorada del ordenamiento jurídico?

En una breve referencia histórica sobre el tema del delito informático se puede afirmar que todo el estudio sobre este tema comenzó en la década de los setenta. Es a partir de mediados de esta década cuando se comienzan a plantear las consecuencias o implicaciones jurídico penales que surgen del abuso o uso abusivo de los sistemas informáticos. Posteriormente en la década de los ochenta se han perfilado con mayor precisión los problemas jurídicos que plantea la delincuencia informática y se ha producido el desarrollo de una legislación específica, en algunos países, que contempla la regulación penal de estas conductas. Las organizaciones internacionales no han dejado de lado este tema y así es importante resaltar la Recomendación del Consejo de Europa número R(89)9 sobre la criminalidad en relación con el ordenador.

La delincuencia informática surge desde el momento en que el uso de los sistemas informáticos abre nuevas vías de ataque a bienes jurídicos ya conocidos y protegidos.

Los sistemas informáticos con su peculiar método de trabajo crean situaciones, supuestos fácticos, totalmente desconocidos para el derecho en general y para el penal en especial. Se puede

producir el ataque a un bien jurídico ya conocido como puede ser la propiedad, pero por unos flancos totalmente desconocidos. Se trata por tanto de identificar esos flancos, o vías de ataque y estudiar si son merecedoras las conductas que utilicen esa vía de ataque de una reprobación penal. Habrá de identificarse dónde o hasta dónde se extiende el bien jurídico protegible (dónde hay propiedad, o intereses patrimoniales individuales) para extender hasta allí la protección penal. Del análisis de las propias características de los sistemas informáticos descubrimos nuevas formas de tratamiento de la información que además de múltiples ventajas aportan nuevas formas, también, para la comisión de delitos[1].

Con estas reflexiones queremos introducir este estudio centrado sobre una de las posibles vías de ataque a la integridad patrimonial del individuo, el fraude cometido por medios informáticos. Por tanto trataremos a los sistemas informáticos y a la informática en general como factores criminógenos, en cuanto medios favorecedores de la comisión de hechos delictivos.

Si los ilícitos informáticos afectan a una doble esfera: la intimidad personal y la integridad patrimonial de la persona (sea ésta física o jurídica), es en esta segunda donde queda subsumida la figura del fraude informático.

Lo específico del delito informático

¿Por qué se puede hablar de delito informático, o de delincuencia informática como una categ[illegible] y no simplemente de *un modo de comisión* de otra forma delictiva antigua ya tipificada? ¿Es que pueden las nuevas tecnologías de la información crear nuevas categorías delictuales autónomas?

Suiza, como apunta Tiedemann[2], se trata de proteger no tanto bienes jurídicos distintos de los ya protegidos, sino objetos concretos[3]. ¿Pero siguiendo esta línea se acabaría negando la existencia del delito informático como categoría independiente? Creemos que no, pero será imprescindible delimitar claramente esos nuevos objetos de protección. A esta tarea fundamental habrá que añadir la de depuración de las figuras delictivas englobadas dentro de la delincuencia informática a través de un proceso de absorción de las versiones nuevas de los delitos antiguos por éstos mismos.

Si este proceso de razonamiento no se admite, hay que concluir que el estudio de las figuras delictivas relacionadas con la informática se justifica únicamente por la estrechez interpretativa que exige el principio de legalidad en materia penal. Y por tanto con una apertura hacia las nuevas formas de comisión a través de medios informáticos de las viejas figuras delictivas desaparecería como categoría independiente la delincuencia informática.

Es, por tanto, tarea fundamental determinar las conductas que son realmente nuevas y que justifican seguir hablando de delincuencia informática, es decir, identificar las nuevas vías de ataque a bienes jurídicos ya protegidos. Delimitar, en suma, lo que más arriba se denominaba nuevos objetos concretos de los tipos penales. Para ello será necesario estudiar las notas que pueden teñir de nuevo y específico una conducta delictiva cometida por medios informáticos. Hay que tras-

---

1 Utilizando un símil el desarrollo de los vehículos de motor supuso un indudable avance para el conjunto de la sociedad, pero también es cierto que se convirtieron en una de las principales amenazas a la integridad física del individuo. Se hizo necesaria una adecuada regulación que estableciera los márgenes de seguridad exigibles en el tráfico de estos vehículos.

2 TIEDEMANN. *Lecciones de Derecho Penal Económico (comunitario, español, alemán)*. PPU. Barcelona. 1993. Pág. 33.

3 Es decir puede existir una extensa legislación penal protectora del derecho de propiedad, como efectivamente así ocurre (Título XIII del Libro 2.º del C. Penal de 1973 define y pena los delitos contra la propiedad en sus diez capítulos. La terminología de delitos contra la propiedad ha sido criticada por parte de la doctrina prefiriéndose la expresión delitos patrimoniales) y sin embargo no ser adecuada para la protección específica de un objeto de propiedad singular como puede ser una línea de comunicación.

cender el medio, hay que ir más allá del medio; el medio, la forma (de comisión) no es substrato lo suficientemente fuerte para hablar de nuevos delitos, de nuevas figuras delictivas. ¿Qué es estonces lo que permitirá hablar de esos nuevos delitos?

Para Nimmer[4] hay que partir de las propias, en cuanto específicas, características del sistema informático para de este modo encontrar la especificidad del delito informático.

Problemas jurídicos para aceptar la categoría delictiva independiente del delito informático

Hasta que no se produzca una reforma en nuestro Derecho Penal positivo que regule la nueva realidad social de los ilícitos informáticos sólo podremos utilizar estas expresiones[5] desde un punto de vista formal no material. Se deben tener en cuenta el Anteproyecto de nuevo Código Penal de 1992, el subsiguiente Proyecto del 92 y el Anteproyecto del 94. Por primera vez, en el Anteproyecto del 92, se recogen en la legislación penal española de forma expresa conductas delictivas relacionadas directamente con los sistemas informáticos. Haciendo un somero repaso a los intentos de modificación de nuestra legislación penal en la materia de la delincuencia informática encontramos cómo los textos de 1980 y 1983 no dedicaban especial atención al tema de la delincuencia informática. Así concretamente la PANCP (Propuesta de Anteproyecto de Nuevo Código Penal) de 1983 en su artículo 189 recogía la respuesta penal a los atentados a la intimidad provenientes del ámbito de la informática, pero descartaba cualquier implicación o ataque que ésta pudiera infringir en la espera patrimonial del individuo.

Por el contrario el Anteproyecto de Nuevo Código Penal de 1992, el Proyecto del 92 y el Anteproyecto del 94 sí contemplan en su articulado una regulación más acabada del fenómeno de la delincuencia informática.

Recogen estos documentos una serie de conductas en las que la informática unas veces se perfila como objeto del ataque delictivo y en otras se convierte en el instrumento de ese ataque. Instrumento de ataque que puede afectar tanto a la intimidad como al patrimonio del individuo. Se enmarca, por tanto, esta posible futura legislación dentro de una concepción amplia de la delincuencia informática.

Ahora intentaremos, partiendo de la teoría jurídica del delito, estudiar la adecuación o acomodación de las conductas englobadas dentro de esa expresión de «delito informático» a la estructura material y moral del delito.

Es decir, se tiende a estudiar y determinar si los requisitos jurídicos que debe reunir un hecho para conceptuarlo jurídicamente como delito pueden cumplirse o se cumplen en las conductas denominadas ilícitos informáticos.

Estos requisitos para los penalistas clásicos como Carrara son: un elemento objetivo, es decir, un acto humano manifestado en el exterior y un elemento subjetivo o psíquico, lo que en derecho penal se denomina acto culpable. Ambos elementos se cumplen al menos en la mayoría de las acciones que estudiamos. Dejamos fuera de nuestro ámbito de atención aquellas conductas producidas sin intencionalidad, sin consciencia, como son intrusismos fortuitos en sistemas de procesamiento de datos, y todas aquellas conductas viciadas por error.

Para la doctrina italiana entre la que cabe destacar a Behemero en la conducta delictiva han de distinguirse tres elementos fundamentales:

---

[4] NIMMER, R. T., *The Law of Computer Technology*. New York, 1985.

[5] Criminalidad informática y delicuencia informática.

1.º La contradicción con el derecho, es decir, la antijuridicidad. No parece difícil argumentar la naturaleza antijurídica de las acciones que se estudian, que habitualmente proporcionan pingües beneficios detrayéndolos ilícitamente de sus legítimos dueños, sean éstos personas físicas o jurídicas. Aunque como pone de manifiesto González Rus[6] parece que muchos de estos delincuentes de «cuello blanco» se ven afectados por el síndrome de «Robin Hood», es decir, legitiman el ataque al patrimonio de una persona jurídica, en cuanto ente jurídico no físico, y reprueban el ataque a la persona física concreta.

2.º El contenido interno, psíquico o culpabilidad. Elemento que se reconoce fácilmente en estas conductas aunque hay que tener en cuenta la existencia de conductas no dolosas sino culposas o incluso fruto de un error. En su caso estos diferentes grados de culpabilidad deberán reflejarse en una atenuación o agravación de la pena correspondiente.

3.º La acción debe ser merecedora, acreedora de una pena, esto es, punible.

Posteriormente la doctrina más consolidada da al concepto del delito una mayor complejidad y añade dos notas más: la tipicidad y condiciones objetivas de punibilidad.

¿Dónde encontramos un obstáculo que nos impide hablar con rigor de conductas delictivas? Es evidente que en la tipicidad. Las conductas englobadas dentro del concepto de criminalidad informática no ofrece duda, son antijurídicas, culpables, concurren las circunstancias objetivas de punibilidad, merecedoras de una pena, pero no existe tal pena puesto que no están tipificadas, no son conductas típicas recogidas y reflejadas como tal en el Código Penal o en Legislación penal especial.

La falta de tipicidad impide hablar de delitos informáticos y deja inmersas estas acciones en la nebulosa de los indiferentes penales.

Concretando ahora el sistema jurídico del delito en el derecho penal español, nuestro Código Penal recoge en su artículo 1 que «son delitos o faltas las acciones u omisiones dolosas o culposas penadas por la Ley».

Si analizamos la definición legal del delito descubrimos las siguientes características: acto externo, positivo o negativo (hacer o no hacer), típicamente antijurídico, culpable y punible.

De todas estas características la que supone, al menos en la actualidad un escollo insalvable es la expresión «penadas en la ley». La antijuridicidad típica se encierra en la expresión «penadas en la ley». «Sólo lo definido en la ley es penalmente ilícito»[7].

A continuación la pregunta a plantearse es ¿qué mecanismo de técnica-jurídica ha de adoptarse para reprimir penalmente los ilícitos informáticos? Siguiendo a Aldama Baquedano[8] se pueden sintetizar las posturas al respecto en dos grandes grupos. Primero: los que entienden que es más conveniente tipificar una única figura de delito informático concediendo, así, un tratamiento unitario a estas conductas. Segundo: los que entienden que establecer un único delito informático es una solución demasiado rígida y deben, «convivir» armónicamente. Para Aldama Baquedano el nuevo tipo penal de delito informático debe configurarse sobre la base de aquellas conductas que utilicen «como medio principal, de manera esencial y necesaria los medios informáticos para fines delictivos». Aquellas otras conductas que no utilicen como medio principal de comisión la informática serán castigadas con arreglo a los tipos tradicionales en los que se haya hecho una referencia a los medios informáticos como medios que agravan la pena a imponer.

Otra solución que se podría proponer en estos temas, en la misma línea de argumentación, sería

---

6 González Rus, Juan José. *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos.* Revista de la Facultad de Derecho de la Universidad Complutense. N.º 12. Monográfico sobre Informática y Derecho. Madrid. Septiembre 1986. Pág. 111.

7 Conde-Pumpido Ferreiro, Cándido. Derecho Penal. Parte General. Editorial COLEX. Madrid. 1990. Pág. 97

8 Aldama Baquedano, Concepción. *Los medios informáticos. (Su utilización al servicio de la Administración de Justicia). (Su utilización perversa o abusiva como medios de vulneración de bienes jurídicamente protegidos).* Poder Judicial nº 30, junio 1993. Página 9 y ss.

considerar como delitos informáticos en sí unicamente aquéllas acciones delictivas que tienen por objeto la **agresión a la información.** La información en cualquier estado en que ésta se encuentre: en proceso, almacenada, en tránsito, etc... Si la comisión del delito se ha producido por medios informáticos estas conductas deben tipificarse con arreglo al delito tradicional más cercano que abarque todo el desvalor de la acción cometida, con la referencia expresa en el tipo penal de «cometido por medios informáticos»[9].

Esta solución propuesta es una de las posibles vías de esclarecimiento del oscuro problema que hoy representa la represión penal de los ilícitos informáticos.

Otra cuestión destacable es la referente al sistema de incriminación que se adopte para otorgar una respuesta penal a estas conductas. Ya se ha visto como *de lege ferenda* nos encontramos ante conductas penalizables, por su alto contenido antisocial y por las graves consecuencias perjudiciales que pueden producir. Pero si *de lege data* la configuración típica como delito de estas conductas, de momento, no existe. Determinar cuándo nos encontramos con la utilización del medio informático para la comisión de un delito ya tipificado y, cuándo con un tipo delictivo independiente de delito informático, es una tarea hoy por realizar y con una dificultad dogmática considerable.

Quizá, insistimos, sea la tipificación de un delito informático en el que el bien jurídico protegido sea de información en proceso y junto a este delito una pléyade de delitos tradicionales con la referencia *cometido por medios informáticos,* una solución aceptable[10].

Contenido del delito informático

Ha de tenerse en cuenta que las nuevas técnicas informáticas no son simplemente el instrumento para la comisión de un delito, sino que en muchas ocasiones son el mismo objeto de la conducta delictiva. Piénsese, por ejemplo, en ataques a los componentes físicos de un sistema de ordenador (de un sistema de proceso de datos) o bien de ataques a los componentes lógicos del sistema, ya se trate de programas informáticos o de datos. De acuerdo con este planteamiento el espectro de conductas calificables de crimen informático es amplísimo. La cuestión fundamental es encontrar el criterio delimitador para esta categoría de conductas. Como pone de relieve Romero Casabona[11] las nuevas tecnologías informáticas deben ser reducidas a sus justos términos. No se puede mantener que una conducta delictiva por el mero hecho de que en ella intervenga un elemento del ámbito de responsabilidad de la informática, es ya delito informático. Si se mantiene esta postura se acabaría considerando cualquier conducta delictiva en la que se vea implicado un ordenador, como un delito informático.

Lo realmente específico en la delincuencia informática lo constituyen las funciones de procesamiento, transmisión y ejecución de programas propias del ordenador. Con esto eliminamos del ámbito de la delincuencia informática todas aquellas conductas que no afecten a alguna de las funciones citadas. Una conducta delictiva

---

[9] Se trataría por tanto de establecer una tipificación especial para el delito de estafa informática, delito de daños a elementos informáticos, ataque a la intimidad a través de los medios informáticos. Los delitos propiamente informáticos serían los que produjeran ataques a la información. Este delito informático, propiamente dicho, entraría, con frecuencia, en concurso con algunos de los delitos tipificados como cometido por medios informáticos.

[10] El bien jurídico atacado y consecuentemente protegido será el que determine la aplicación del tipo específico del delito informático o la de otro tipo tradicional. Teniendo en cuenta que en muchos casos se producirá un concurso delictual entre el denominado delito informático independiente y uno de los tipos tradicionales cometido por medios informáticos. Por ejemplo una manipulación en el proceso de los datos dentro de una entidad financiera que produce un beneficio al autor del hecho. La conducta supone una agresión de la información en proceso y constituye por la forma de comisión, el resultado, etc... un delito de estafa informática.

[11] Romeo Casabona, Carlos María. *Poder informático y seguridad jurídica.* Fundesco. Madrid 1987. Pág. 41.

aunque se encuentre vinculada con las nuevas tecnologías de la información, si no se produce esa vinculación también respecto del procesamiento, de la transmisión o del uso de un programa, no puede incluirse dentro del ámbito de la delincuencia informática.

El Prof. Davara adelantándose a una realidad que podremos constatar en breve espacio de tiempo, como es la tipificación en la legislación penal de estas conductas como delitos informáticos, adopta la terminología del delito informático, prescindiendo por tanto del concepto más genérico de criminalidad informática, y los define como: «la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software»[12]. Es, o puede ser, la **informática** tanto **medio** como **objeto** de la agresión ilegítima. Agresión que puede afectar a bienes patrimoniales o a la intimidad de los individuos. Confluyen así, en esta definición sincrética, todas las precisiones que cabe hacer en relación con el contenido de la categoría del delito informático.

El fraude informático dentro de la criminalidad informática

No es difícil encontrar autores que no distinguen el ilícito informático en general del fraude informático en especial. El fraude informático es una parte de un todo que es el ilícito informático.

La utilización de la expresión «fraude informático» no es una cuestión pacífica ni generalmente aceptada[13]. Se utilizan otras aunque en definitiva no sean sino subformas de la más general que es el fraude. Algunas de estas expresiones alternativas son las siguientes: manipulación de datos, ilícitos patrimoniales por medios informáticos, estafa informática.

En opinión de Gutiérrez Francés la expresión «fraude informático» no es, primero, ni una categoría jurídico-positiva, ni, segundo, tampoco tiene contenido rígido. La primera apreciación se explica al no existir como tal tipo penal en la legislación positiva y la segunda al constatar la amplia gama de conductas que podemos situar dentro del fraude informático (estafa informática, falsedades por medios informáticos). Asimismo debemos tener en cuenta la posibilidad de vulnerar bienes de carácter macrosocial a través de los fraudes informáticos, por ejemplo: el fraude fiscal, o el fraude bursátil (contra el sistema de cotizaciones)[14].

Siguiendo con la tarea de delimitación de nuestro ámbito de interés seguiremos a Agustín Domínguez[15] para determinar las características fundamentales del fraude informático:

1.º impacto financiero;

2.º queda involucrado el proceso electrónico de datos en la perpetración del hecho delictivo o en su encubrimiento;

3.º ánimo de engaño.

Para poder hablar con rigor de fraude informático debemos encontrarnos ante una conducta realmente fraudulenta.

Camacho Losa caracteriza el fraude informático como aquel bloque de la delincuencia informá-

---

12 Davara Rodríguez, Miguel Ángel. *Derecho Informático.* Ed. Aranzadi. Pamplona. 1993. Pág. 318.

13 Cfr. Gutiérrez Francés, M.ª Luz. *En torno a los Fraudes Informáticos en el Derecho Español.* Actualidad Informática Aranzadi. N.º 11, abril 1994. Director M. A. Davara. Págs. 7 y ss.

13 Cfr. Gutiérrez Francés, M.ª Luz. *Fraude informático y estafa.* Ministerio de Justicia. Secretaría General Técnica. Centro de Publicaciones. Madrid. 1991. Pág. 89.

15 Domínguez, Agustín. *Transferencia electrónica de fondos y de datos. Protección jurídica de los datos personales emitidos en una operación de pago electrónico.* Encuentro sobre Informática y Derecho 1992-1993. Coordinador: Prof. Dr. D. Miguel Ángel Davara. Ed. Aranzadi. Pamplona 1993. Págs. 117 y ss.

tica integrado por usos indebidos o manipulaciones fraudulentas de elementos informáticos de cualquier tipo que posibilitan un beneficio ilícito[16]. Este autor sistematiza las notas características del fraude informático en los siguientes puntos:

1. Conducta fraudulenta.
2. Utilización de los componentes de un sistema informático.
3. La finalidad que se persigue es la obtención de un beneficio ilícito.
4. Producción de un perjuicio a otro.

Quizá no sea un mal método, *para tomar conciencia del peligro que suponen este tipo de conductas delictivas relacionadas con la informática y para acercarse a la realidad de sus características tratar de extrapolar el ataque a nuestro propio entorno de trabajo. Es decir, hacer un ejercicio de traslación y ver, o intentar ver, el reflejo práctico, las consecuencias, que hubiera tenido el ataque a nuestro sistema informático, del que cada vez con más fuerza dependemos para el desarrollo del trabajo habitual.* En este contexto se puede tomar una idea más exacta de lo que hay que hacer ante una situación semejante. Para ello hemos intentado reflejar en las siguientes páginas algunos casos reales conocidos por la Jurisprudencia de nuestro Tribunal Supremo y que ayudan a apreciar con mayor cercanía el fenómeno del fraude informático. Son ya varias las Sentencias del Tribunal Supremo[17] que han tratado, de momento de modo tangencial, las características específicas del fraude informático. En el substrato de estas declaraciones jurisprudenciales se plantea la siguiente cuestión: ¿Cómo podemos establecer la diferencia entre la figura del fraude informático y la estafa informática, y de esta diferenciación deducir la individualidad e independencia de ambas conductas?

Parece que la noción de fraude lleva consigo la existencia de una relación de poder especial como el «aprovechamiento de las facilidades que proporciona la situación, en este caso de dependencia». ¿Podría por tanto afirmarse que la conducta fraudulenta lleva aparejada, o mejor, supone la existencia de una relación que facilita la comisión de la conducta ilícita? Creemos que sí se puede mantener esta postura, cifrando precisamente en este punto el criterio diferenciador entre el fraude y la estafa. En el fraude el engaño, elemento esencial de la estafa, no es necesario. En el fraude el acceso al objeto de la defraudación ya se tiene libre, expedito, por la relación de confianza o de poder previa existente entre el autor y el medio en el que cometerá la conducta ilícita. Sólo falta provocar el error, a través de la manipulación, y consecuentemente la disposición patrimonial en favor del defraudador.

A diferencia de lo visto en el fraude, en la estafa no existe dicha relación especial. En el caso de la estafa un ajeno logra la disposición patrimonial en su favor valiéndose de un engaño que causa error en otro y a falta de relación previa especial acude al engaño. Interpretamos, así, el engaño como la preparación o creación de un espacio de confianza que posteriormente es utilizado torticeramente para obtener un beneficio ilícito. En el fraude ese espacio de confianza ya se encuentra establecido y el delincuente hace un uso indebido del mismo, se aprovecha de él en su propio interés. Como ejemplo de esta interpretación cabe mencionar la Sentencia de 19 de abril de 1991. En esta Sentencia se declara *probado que con fechas anteriores al mes de julio* de 1985, J. V. M. desempeñaba en una sucursal urbana de recogidas del Banco Hispano Americano el cargo de apoderado. El desempeño de este cargo le confería la posibilidad de acceder a las cuentas corrientes de diversos clientes del banco. Aprovechando esta circunstancia manipuló las cuentas corrientes de distintos clientes realizando apuntes inexistentes por vía del ordenador. Con estas operaciones logró trasladar a su patrimonio particular varios millones de pesetas.

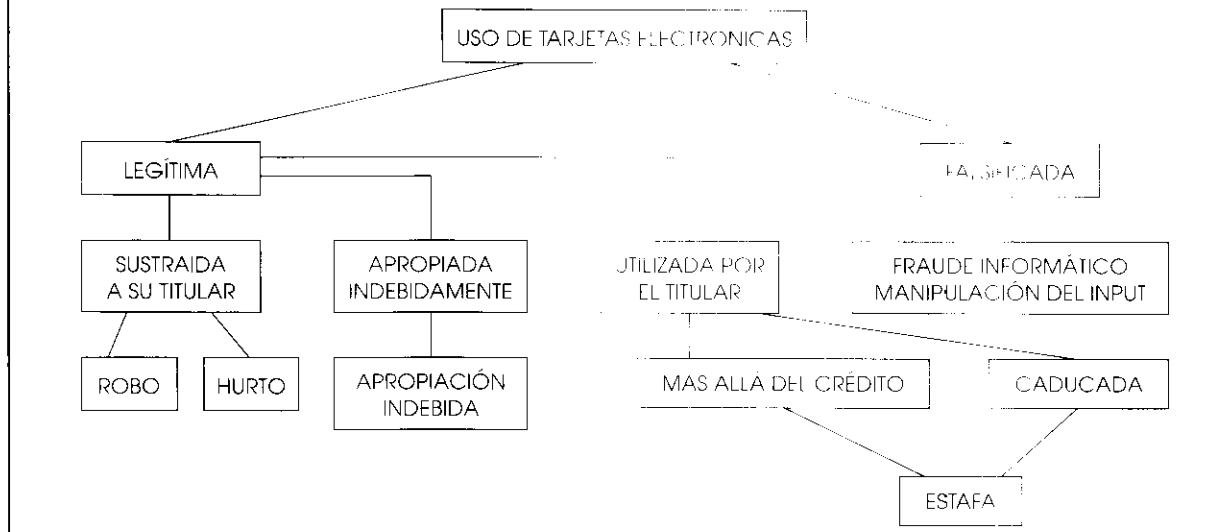
La Audiencia condenó en primera instancia a J. V. M. como autor de un delito continuado de falsedad en documento mercantil y como autor de un delito continuado de estafa apreciando la

---

[16] Camacho Losa, L. *El delito informático*. Madrid. 1987. pp. 25-26.

[17] Sentencia de 14 de enero de 1987, Sentencia de 8 de octubre de 1988, Sentencia de 8 de noviembre de 1989, Sentencia de 5 de diciembre de 1989, Sentencia de 19 de abril de 1991, Sentencia de 16 de septiembre de 1991 y Sentencia de 25 de enero de 1994.

Figura 1. Riesgos de tarjetas electrónicas



agravante específica de especial gravedad por la cuantía de la defraudación[18].

La Sentencia se recurre en casación ante el Tribunal Supremo y este Tribunal dicta segunda Sentencia condenando por un delito continuado de falsedad en documento mercantil[19] y por un delito continuado de apropiación indebida. En esta segunda Sentencia también se aprecia la agravante específica de especial gravedad, en razón por la cuantía de lo apropiado. En la Sentencia dictada en casación por el Tribunal Supremo se produce un *cambio en el título de imputación* al pasar de calificarse los hechos como constitutivos de un delito de estafa, a ser calificados como constitutivos de un delito de apropiación indebida. Este cambio se produce, a nuestro entender, por dos órdenes de razones: primero, se tiene en cuenta la circunstancia personal del autor de los hechos que desempeña el cargo de apoderado del Banco y segundo, el engaño, elemento fundamental en la estafa, no puede afectar a máquinas[20]. La Sentencia continúa diciendo

[18] En este sentido se pronuncia el Prof. DAVARA al decir que «si no son delito determinadas actuaciones dolosas realizadas por medios informáticos, lo cierto es que a través de estos medios existe la posibilidad de causar un mayor daño o mal, atentando en mayor medida contra el bien jurídico protegido». *Derecho Informático*. Op. Cit. Página 335.

[19] La jurisprudencia ha configurado un concepto amplio de documento mercantil. Ante la falta de determinación en el Código Penal vigente del concepto de documento mercantil ha sido la doctrina jurisprudencial la encargada de delimitar esta figura. En primer lugar toca determinar el concepto de documento. Para ello resulta de gran interés la Sentencia del Tribunal Supremo de 5 de febrero de 1988. Ponente: Sr. Ruiz Vadillo. En esta Sentencia, en orden a la determinación de los medios de prueba, se declara que estos medios no están recogidos con carácter exhaustivo en las leyes de procedimiento sino que los nuevos medios técnicos puede «subsumirse en el concepto mismo, amplio desde luego, de documento en cuanto cosas muebles aptas para la incorporación de señales expresivas de un determinado significado». Admite esta Sentencia el carácter de un documento en soporte electrónico como documento jurídicamente válido. Por tanto la manipulación de cuentas corrientes en soporte informático se admite como documento y con el caracter de mercantil al hacer referencia a una operación de comercio o que sirve para demostrar derechos de naturaleza mercantil. La misma Sentencia que se viene comentando de 19 de abril de 1991 acude a un concepto material de documento aceptando como tal los más adelantados y funcionales medios de representación de información. En alusión a los disquetes informáticos como «portadores de manifestaciones y acreditamientos con vocación probatoria». Estos documentos, sigue diciendo la Sentencia, «pueden ser objeto de manipulación igual que un documento escrito.»

[20] En este sentido el Prof. ROMEO CASABONA señala cómo algunos elementos del tipo de la estafa, por ejemplo el engaño y el error, «han de recaer y originarse sucesiva y exclusivamente en un individuo». Las manipulaciones informáticas, de acuerdo con estas conside-

que «la inducción a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina». La aplicación del tipo de apropiación indebida se fundamenta en la circunstancia de que el autor de los hechos desempeña el cargo de apoderado de los fondos que le han sido entregados para su administración. Cumpliéndose así el elemento básico del tipo de apropiación indebida. En definitiva la Sentencia resulta de gran interés al aceptar, por su parte, dentro del concepto de documento a los soportes informáticos, y reconocer su protegibilidad jurídica. Y por otra parte ante una primera calificación de los hechos como constitutivos de un delito de estafa el Tribunal Supremo estima que la aplicación del delito del artículo 528 del Código Penal no es adecuada. La manipulación dolosa de información no se hace aprovechando una relación de poder especial que tiene el autor como apoderado del banco. Así pues la condición de apoderado del autor hace que la estafa no sea el tipo más adecuado para incriminar los hechos y se acuda a otro delito como es la apropiación indebida donde se toma en cuenta la relación especial que liga al autor con la víctima. La creación de un nuevo tipo penal de fraude informático recogiendo las características del tipo de la estafa excepto el engaño sustituído por la exigencia de una relación de confianza quizá ayudaría a resolver el problema de la criminalización de las conductas de fraude informático.

Tipos de fraudes informáticos

Romeo Casabona da una noción, desde un punto de vista eminentemente práctico, de fraude informático hablando de él como de la conducta de manipulación de datos informatizados que alterando el resultado del procesamiento produce un perjuicio a un tercero y a la vez un beneficio, o una posibilidad de beneficio, al autor que actúa con ánimo de lucro.

Sigue diciendo este autor, coincidiendo así con la exposición del Prof. Davara, que estas manipulaciones aludidas tanto pueden producirse en la introducción de los datos, en el programa correspondiente (input), en el programa mismo, o bien en la salida de los datos (output).

Los distintos tipos de manipulaciones a los que hemos hecho referencia merecen una atención particularizada.

1. Las manipulaciones en la entrada de datos («input»). No es otra cosa sino introducir datos falseados en el ordenador. Falseamiento que puede provenir de la modificación de datos reales, de la introducción de datos completamente ficticios o bien de la omisión del registro de datos.

Si la introducción de datos está falseada el resultado también lo estará aunque el proceso llevado a cabo con esos datos haya sido completamente correcto.

Las acciones fraudulentas se dirigen fundamentalmente contra dos objetivos: los datos y los programas informáticos. Los datos tratados por un sistema automatizado se pueden ver afectados por las siguientes agresiones: consulta indebida, apropiación de información, eliminación de datos y la modificación no autorizada de los datos. De acuerdo con la legislación española contra estas agresiones se encuentran protegidos los datos de carácter personal. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[22] recoge una exhaustiva reglamentación sobre el deber de secreto que ampara a los datos personales sometidos a tratamientos automatizados. Del mismo

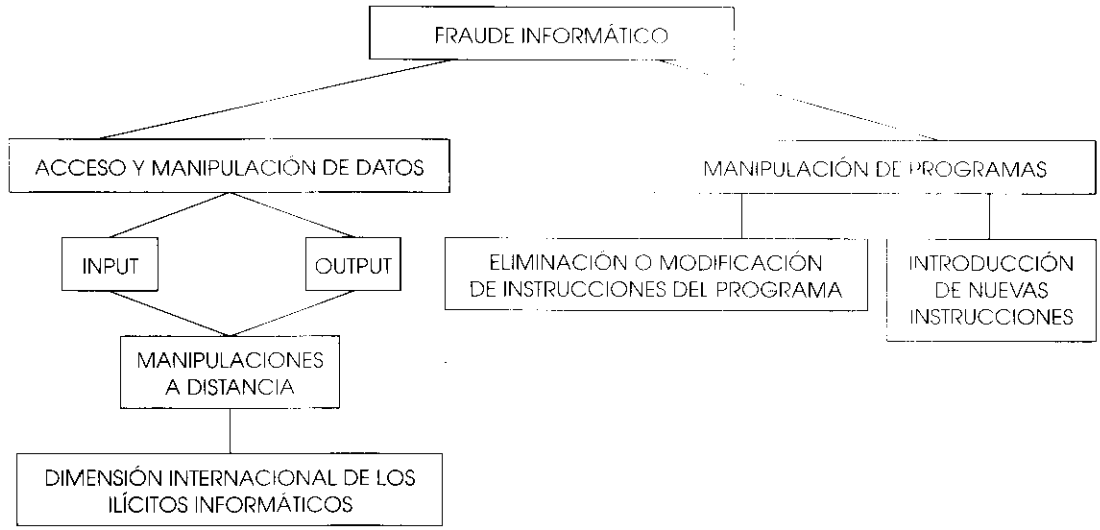
raciones, no reunirán los requisitos para calificarse como estafa al no poder apreciar el engaño sobre una máquina. «El ordenador no puede ser sujeto del engaño en relación con el delito de estafa». Ahora bien, este autor introduce una precisión fundamental: la aplicación del tipo de la estafa a las manipulaciones informáticas depende en gran medida del sistema de trabajo adoptado por la empresa y de los sistemas de control que se siguen en la misma. Si existen una o varias personas que supervisan el proceso que se realiza informáticamente, es sobre estas personas sobre las que se podrá apreciar la incidencia del engaño. ROMEO CASABONA, CARLOS MARÍA. *Poder Informático y Seguridad Jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información.* FUNDESCO. Madrid. 1987. Pp 58 y ss.

21 ROMEO CASABONA, C. M. *Poder informático y seguridad jurídica.* Fundesco. 1988. Pp. 47 y ss.

22 BOE, 31 de octubre de 1992 (núm. 262).

Del mismo modo reconoce, en su artículo 17.1[23], la tutela de los derechos del titular de los datos ante la Agencia de Protección de Datos. Este artículo 17 de la Ley Orgánica 5/1992 ha sido desarrollado, a su vez, por el artículo 17 del Real Decreto de 29 de junio de 1994[24]. Resulta, así mismo, muy rigurosa la sanción que prevé el artículo 16[25] del Real Decreto 1332/1994 para los datos que hayan sido recogidos o registrados por medios fraudulentos.

Figura 2. Tipos de fraudes informáticos



Vemos como el legislador español no es ajeno a la compleja problemática de la manipulación de datos sino que, muy al contrario, establece sanciones y medios de defensa precisos a los afectados por una manipulación de este tipo.

Por otra parte decíamos que el segundo objeto de ataque lo constituían las aplicaciones informáticas o programas informáticos. Un programa informático puede verse agredido por tres tipos de acciones: accesos indebidos, apropiación indebida para uso y comercialización y modificación de la aplicación. Es, dentro de las tres acciones descritas, la modificación del programa la forma más común de comisión de fraudes informaticos. La protección de la integridad del programa viene reconocida en derecho español por el Título VII del Libro I de la Ley de Propiedad Intelectual de 11 de noviembre de 1987 y por la Ley de incorporación al derecho español de la Directiva 91/250/CEE, de 14 de mayo (LCEur. 1991, 475), sobre la protección jurídica de programas de ordenador, de 23 de diciembre de 1993, núm. 16/1993. Ambas leyes someten a la autorización del autor del programa cualquier reproducción,

[23] «Artículo 17. Tutela de los derechos y derecho de indemnización.
1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamacion por los afectados ante la Agencia de Protección de Datos en la forma que reglamentariamente se determine».

[24] Real Decreto 20 de junio de 1994, núm. 1332/1994. Desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre (RCL 1992, 2347), de regulación del tratamiento automatizado de los datos de carácter personal. BOE, 21 de junio de 1994 (núm. 147).

[25] «Artículo 16. Bloqueo de datos.
... el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.»

transformación o distribución del mismo. No son menos importantes las medidas que recogen de lucha contra la piratería informática. La ley del 93 recoge como medio eficaz para combatir la piratería la posibilidad que se le da al juez en el artículo 9 para que, previamente a la adopción de las medidas cautelares, pueda requerir los informes u ordenar las investigaciones que estime oportunas, a fin de obtener las pruebas necesarias para el procedimiento.

Vemos por tanto como la legislación española reconoce la antijuridicidad de las acciones de manipulación de datos y programas y sanciona estas conductas.

2. Manipulaciones en el programa.

La entrada de datos es correcta pero una manipulación de procesamiento conduce a la obtención de resultados falsos. Las manipulaciones de los programas pueden ser variadas: la alteración de una o varias instrucciones, la supresión de una o varias de estas instrucciones, adición de nuevas instrucciones, inversión del orden de las instrucciones. Junto a estas manipulaciones que inciden directamente sobre el programa es interesante también tener en cuenta aquéllas que actúan sobre los datos que el programa toma como constantes para la realización de un cálculo determinado.

Estas manipulaciones se realizan, normalmente, con las pertinentes medidas de ocultación que evitan el descubrimiento de la manipulación e incluso devuelven al programa a su estado original.

3. Manipulaciones en la salida de los datos («output»).

Se trata de modificaciones de los datos de salida, de los resultados del procesamiento. Quizá sean éstas manipulaciones más sencillas de efectuar.

4. Manipulaciones a distancia.

Si las manipulaciones descritas hasta ahora se realizan normalmente por empleados de la misma empresa o entidad que las sufre y se encuentran en el mismo recinto, nada empece a que se realicen a distancia si los ordenadores en los que se encuentran los datos y programas objeto de la agresión se encuentran conectados a través de una línea de comunicación.

Implicaciones internacionales de las acciones de fraude informático

Es en relación con las manipulaciones a distancia donde se introduce un problema de máximo interés y complejidad: la dimensión internacional que en muchas ocasiones adquieren los delitos informáticos. No se debe olvidar que los elementos de un sistema informático en muchas ocasiones se encuentran dispersos en el espacio, geográficamente distantes, y son múltiples las conexiones entre sistemas informáticos de diferentes Estados.

Si los problemas en relación con las implicaciones jurídico-penales en el uso de los sistemas informáticos (las manipulaciones de datos y programas antes estudiadas) encuentran difícil respuesta, o adecuado tratamiento, en el ámbito de derecho interno, la situación se complica si el supuesto de hecho que contemplamos afecta a diversos Estados. Si las soluciones no son claras en la legislación de un Estado no ayuda en nada que en el supuesto fáctico se hallen implicados varios países. Más bien lo que esto determina es la aparición de nuevos problemas. En la identificación de éstos creemos conveniente hacer referencia al estudio de Vilariño Pintos[26] donde quedan planteadas las cuestiones fundamentales del problema. Primero la determinación del lugar de la comisión de una manipulación de datos o de

26 VILARIÑO PINTOS, EDUARDO. *El delito informático. Derecho comparado y aspectos jurídico-internacionales.* En vol. *Hacia un Nuevo Orden Internacional y Europeo.* Editorial TECNOS. Pp. 807 y ss.

programas informáticos cuando los hechos se han realizado en distintos Estados. Para Vilariño este tipo de actos deben recibir un tratamiento similar al otorgado a los denominados por la doctrina penal «delitos a distancia» siguiéndose la «teoría de la ubicuidad» para su adecuada incriminación penal. De acuerdo con esta teoría se considera cometido el hecho en todos los lugares donde se realizan actos o se producen efectos pertenecientes al tipo penal positivamente regulado.

Una segunda cuestión que debe tenerse en cuenta es la determinación del foro competente para el conocimiento de estos hechos. En este punto Vilariño sigue abogando por la aplicación de la misma teoría de la ubicuidad. Esta teoría, dice este autor, asegura una mayor eficacia en la perseguibilidad del delito. Así es realmente, ya que de acuerdo con ella puede conocer de los hechos cualquier Tribunal perteneciente a uno de los Estados donde se haya realizado alguno de los hechos integrantes del delito o se hayan producido sus efectos. El derecho aplicable será el del foro, teniendo en cuenta la tremenda descoordinación, falta de homogeneidad, que entre las distintas legislaciones nacionales existe sobre estos temas y el absoluto vacío legal que en muchas de ellas se aprecia, la respuesta judicial que se dé a unos mismos hechos dependiendo del Tribunal que de ellos conozca puede llegar a ser absolutamente dispar.

Este problema es vislumbrado por Vilariño y por ello defiende la configuración de estas conductas con implicación internacional como delitos de derecho internacional regidos por un convenio específico que permita un tratamiento adecuado y uniforme de la delicuencia informática internacional.

Por último y para asegurar una mayor eficacia en la perseguibilidad de las manipulaciones a distancia y asumiendo la configuración de estas conductas como delitos de derecho internacional estamos de acuerdo con Vilariño en la adopción del criterio de la competencia universal. De acuerdo con él cualquier Estado firmante del convenio internacional específico sobre criminalidad informática que aprehenda en su territorio al presunto autor o autores de una de estas manipulaciones, podrá proceder a su enjuiciamiento.

En definitiva no se trata sino de extender, con este criterio de la competencia universal, el ámbito de conocimiento con similar flexibilidad y facilidad que para la comisión de los hechos delictivos proporcionan los sistemas telemáticos.

Seguros contra fraude informático

La concienciación creciente de las empresas en relación con la consideración de la información que manejan como un activo más ha determinado, en época reciente, la aparición de una nueva póliza de seguros para cubrir las pérdidas ocasionadas por la manipulación fraudulenta de los datos objeto de tratamiento automatizado.

Este seguro se oferta en España con el nombre de «Seguro contra el fraude por ordenador». Debe hacerse constar que todavía no cuenta con una amplia implantación en el sector asegurador español, e incluso algunas grandes compañías aseguradoras lo desconocen por completo. Pero, puede decirse que, empieza a despertarse en los clientes el interés por esta cobertura por lo que pasamos a exponer las características más sobresalientes de estas nuevas pólizas.

El seguro de fraude informático cubre contra los siguientes riesgos:

1. Transmisión, entrega de fondos o propiedades, etc. como resultado directo de una introducción fraudulenta de datos electrónicos.
2. Seguro de instrucciones electrónicas para ordenador.
3. Seguro de datos y medios electrónicos.
4. Seguro de comunicaciones electrónicas.
5. Seguro de operaciones de la oficina de servicios del asegurado.
6. Seguro de transmisiones electrónicas.

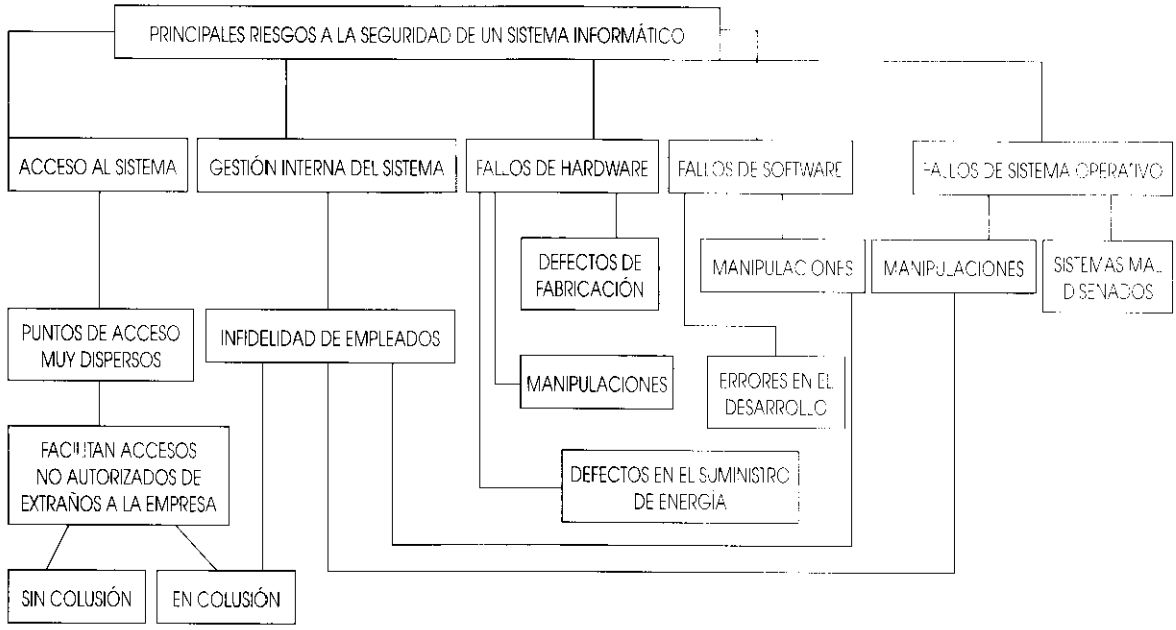
Vemos como quedan incluídas las formas de fraude más típicas. El asegurador cubre practicamente todos los riesgos derivados de una acción fraudulenta. Sin embargo esta cobertura no es aconsejable sin que la compañía aseguradora tome una serie de precauciones.

Un problema fundamental que se plantea en este tipo de seguro es el de cuantificar la cobertura del mismo. Para salvar este inconveniente las aseguradoras que ofrecen esta cobertura exigen del cliente un estudio previo sobre las medidas de seguridad adoptadas en su empresa, la historia de anteriores acciones fraudulentas sufridas, etc. Si la aseguradora entiende que estas medidas de prevención no son las adecuadas exige que se adopten las medidas de seguridad necesarias para minimizar al máximo el riesgo de fraude.

global de bancos y su finalidad es proporcionar una cobertura contra los delitos relacionados con la informática que normalmente se excluyen de la póliza global de bancos.

La casi totalidad de las empresas aseguradoras no venden una póliza de seguro de criminalidad informática o de fraude informático sin que previamente exista la cobertura de daños materiales. Las razones que se esgrimen para explicar esta situación son dos: por una parte para las coberturas nuevas, que son más peligrosas que el seguro de daños materiales, es necesario lograr un equilibrio de riesgo. La prima del seguro de daños materiales facilita este equilibrio. La segunda razón es puramente comercial. Una forma de aumentar la cartera del seguro de daños materiales es incluir nuevas coberturas (fraude informático) en un paquete amplio de daños materiales facilita este equilibrio.

Figura 3. Riesgos de un sistema informático



La póliza de fraude por ordenador está diseñada en la mayoría de las compañías aseguradoras como una póliza complemento de la póliza

Dado que todavía no se encuentra muy extendida como póliza independiente la de fraude informático resulta interesante comprobar cómo en

la práctica se está dando respuesta desde el sector asegurador a este tipo de riesgos con las coberturas proporcionadas por otro tipo de pólizas: las de infelidad de empleados.

Habiéndose constatado en la realidad que son en la mayoría de las ocasiones los «insiders», es decir, los propios empleados de la empresa defraudada los autores del fraude se ha considerado más conveniente acudir a un tipo de póliza que ya cuenta con amplia tradición en nuestro mercado asegurador para cubrir estos riesgos. En las pólizas de infidelidad de empleados la compañía aseguradora se compromete a pagar al asegurado todas las pérdidas directas que sufra durante el período descubierto debido a acto o actos de fraude o deshonestidad cometidos por cualquier empleado mientras está a su servicio, por un importe que no supere la prima asegurada.

Por empleado se entiende cualquiera o todas las personas que están contratadas al servicio del asegurado en el ejercicio de su negocio. Inmediatamente después del descubrimiento de cualquier acto o actos de fraude o deshonestidad por cualquier empleado el asegurado debe hacer notificación escrita a la compañía. Se excluyen de la cobertura los fraudes descubiertos después de los 12 meses siguientes a la dimisión o cese del empleado.

Por último conviene aquí hacer referencia a una nueva forma de contratos informáticos que por la vía de la reparación financiera pretende mantener la actividad empresarial en el caso de que circunstancias previstas pero inevitables (podría aquí entenderse incluidas las acciones de fraude informático) impidan seguir con el funcionamiento normal del sistema informático. Nos estamos refiriendo al contrato de Back-Up[27]. Se trata de una medida de aseguramiento que en algunos casos se configura como un contrato de seguro.

Conclusiones

Como conclusiones de la investigación desarrollada en relación con el riesgo procedente de una acción de fraude informático queremos hacer las siguientes precisiones:

1.º Entendemos que, pese a la incriminación o penalización de las conductas de fraude informático como constitutivas de un delito de estafa por la mayoría de la jurisprudencia del Tribunal Supremo español, no es adecuado el tipo de estafa para abarcar todo el desvalor de estas conductas por varias razones. Primero en las acciones de fraude no existe un engaño sino un aprovechamiento de una relación de confianza entre defraudador y defraudado que utiliza aquél para cometer la acción delictiva. Entendemos que el desvalor que supone traicionar una relación de confianza preexistente es superior a la provocación de un engaño. Segundo, si el engaño es elemento fundamental, columna vertebral, de la estafa es realmente difícil aceptar que se pueda engañar a una máquina, tesis que deben sostener los partidarios de la aplicación del tipo de la estafa a los fraudes informáticos, cuando una máquina no tiene conciencia ni voluntad.

2.º Si la respuesta penal que hoy cabe dar con el Código Penal español en la mano no nos satisface ¿qué solución debe arbitrarse? A nuestro entender ha de adoptarse una postura audaz. La solución vendría no tanto por la tipificación de un nuevo delito de estafa informática, solución que adopta el Anteproyecto de Código Penal del 94, sino por el reconocimiento de un nuevo bien jurídico penalmente protegido: EL PROCESAMIENTO ELECTRÓNICO DE LA INFORMACIÓN. La protección del tratamiento automático de la información frente a los constantes ataques a los que se puede ver sometido es actualmente nula

27 DEL PESO NAVARRO, EMILIO. *Los contratos informáticos y la contratación electrónica*. Curso de Derecho Informático e Informática Jurídica. Instituto de Informática Jurídica. Facultad de Derecho. Universidad Pontificia Comillas. ICADE. 1994.

o existente en el derecho penal español, no así en otras ramas del derecho (Protección de datos, propiedad intelectual...) que ya hemos visto, sí otorgan dicha protección.

3.° Esperamos que el momento que actualmente atraviesa nuestra legislación penal de profunda reforma sea aprovechado para introducir el reconocimiento de estos nuevos bienes jurídicamente protegibles.

4.° Mientras la adecuada respuesta penal al tema del fraude informático llega, el mundo empresarial comprende la necesidad de cubrir el riesgo al que diariamente se expone de sufrir manipulaciones fraudulentas de sus sistemas informáticos. De este modo se presenta hoy la vía de la reparación financiera como la solución más adecuada. Bien con la retención del riesgo en la figura del autoseguro, o bien a través de la suscripción de una de las nuevas pólizas contra fraude informático es como se puede lograr un mejor sistema de cobertura frente a una acción defraudatoria.

5.° Por último debemos decir que si nuestro Código Penal es una de las normas que refleja el orden valorativo de una determinada sociedad, la sensibilidad dominante en el ámbito empresarial español reclama la configuración de unos nuevos tipos penales presididos por el principio de defensa de uno de los activos, hoy, más valiosos en cualquier empresa: EL PROCESAMIENTO AUTOMÁTICO DE SU INFORMACIÓN. ■