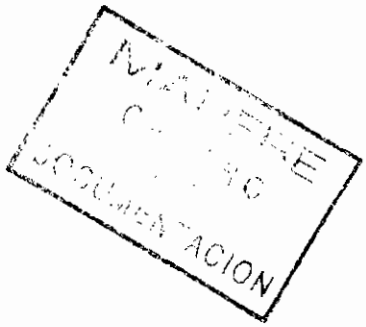
NI 77882
R 14714
R. 23208



CUADERNOS DE LA FUNDACION

Nº 35

* * * * * * *

EL CONTROL DE RIESGOS EN FRAUDES INFORMÁTICOS

Autor: Juana María Domaica Maroto

junio, 1997

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ISBN: 84-89429-18-9

Depósito Legal: M-20.018-1997

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

LISTA DE CUADERNOS DE LA FUNDACION MAPFRE ESTUDIOS EDITADOS:

1. Filosofía Empresarial
2. Resultados de la Encuesta sobre "Altos Profesionales de Seguros" (A.P.S.)
3. Dirección y Gestión de la Seguridad
4. Los Seguros en una Europa cambiante: 1990-1995 (No disponible)
5. La Distribución Comercial del Seguro: Sus Estrategias y Riesgos
6. Elementos de Dirección Estratégica de la Empresa
7. Los Seguros de Responsabilidad Civil y su Obligatoriedad de Aseguramiento
8. La Implantación de un Sistema de Controlling Estratégico en la Empresa
9. Técnicas de Trabajo Intelectual
10. Desarrollo Directivo: Una Inversión Estratégica
11. El Concepto de Seguridad en la Ciencia y la Ciencia de la Seguridad
12. Los Seguros de Salud y la Sanidad Privada
13. Calidad Total y Seguridad
14. El Reaseguro de Exceso de Pérdidas
15. El Coste de los Riesgos en la Empresa Española 1991
16. La Legislación Española de Seguros y su Adaptación a la Normativa Comunitaria

Número Especial: Informe sobre el Mercado de Seguros 1993

17. Medio Ambiente Seguro: Desarrollo Futuro
18. El Seguro de Crédito a la Exportación en los países de la OCDE (Evaluación de los resultados de los aseguradores públicos)
19. Una Teoría de la Educación
20. El Reaseguro en los Procesos de Integración Económica

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Número Especial: Informe sobre el Mercado de Seguros 1994

21. La Nueva Regulación de las Provisiones Técnicas en la Directiva de Cuentas de la C.E.E.
Provisiones Técnicas de Seguros de Vida en las Directivas Comunitarias

22. Rentabilidad y Productividad de Entidades Aseguradoras

23. Análisis de la Demanda de Seguro Sanitario Privado

24. El Seguro: Expresión de Solidaridad desde la Perspectiva del Derecho

25. El Reaseguro Financiero

26. El Coste de los Riesgos en la Empresa Española 1993

27. La Calidad Total como Factor para elevar la Cuota de Mercado en Empresas de Seguros

28. La Naturaleza Jurídica del Seguro de Responsabilidad Civil

29. Ruina y Seguro de Responsabilidad Civil Decenal

Número Especial: Informe sobre el Mercado de Seguros 1995

30. El Tiempo del Directivo

31. Tipos Estratégicos, Orientación al Mercado y Resultados Económicos: Análisis Empírico del Sector Asegurador Español

32. Decisiones Racionales en Reaseguro

33. La función del Derecho en la Economía

34. El Coste de los Riesgos en la Empresa Española 1995

35. El Control de Riesgos en Fraudes Informáticos

Copyright: F.M.E.
Prohibida la reproducción total o parcial de este trabajo sin el permiso escrito del autor o de la FUNDACION MAPFRE ESTUDIOS.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

PRESENTACIÓN

La informática se ha convertido en la herramienta de gestión más poderosa al alcance de la empresa. La extensión de su uso público, combinado con la multiplicidad de canales de información, hace que los denominados "riesgos informáticos" se multipliquen.

La autora, que disfrutó de una beca de investigación "Riesgo y Seguro" de la Fundación, aborda con rigor el tratamiento y gestión de estos riesgos desde su tipificación hasta los sistemas de control y aseguramiento.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

EL CONTROL DE RIESGOS

EN FRAUDES INFORMÁTICOS

Autor: Juana María Domaica Maroto

Abogado

Graduado Superior en CC. Jurídicas (ICADE)

Trabajo resultante de una Beca Riesgo y Seguro 1993-94, concedida a la autora por la Fundación MAPFRE Estudios.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ÍNDICE

PÁGINA

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

PÁGINA

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

PÁGINA

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

PÁGINA

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

EL CONTROL DE RIESGOS EN FRAUDES INFORMÁTICOS

Autor: Juana María Domaica Maroto

Abogado

Graduado Superior en CC. Jurídicas (ICADE)

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

INTRODUCCIÓN

A lo largo de las páginas de este trabajo se ha pretendido analizar, desde una perspectiva jurídica, una realidad que ha ido creciendo y desarrollándose de forma paralela a la extensión e implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en nuestra vida de relación, nos referimos a las conductas delictivas relacionadas con las TIC.

Dentro del amplio espectro de estas conductas sólo aquellas en las que la manipulación de un sistema o de un proceso informático ha producido un desplazamiento patrimonial en favor del autor de la manipulación y en perjuicio de un tercero (ya sea el dueño del sistema o un tercero) han constituido el objeto central de investigación y análisis.

La aprobación por Ley Orgánica 10/1995, de 23 de noviembre, del nuevo Código Penal español ha dado acogida a nuevas formas de delincuencia, introduciendo entre los delitos contra el orden socioeconómico el de estafa producida mediante manipulación informática o artificio semejante. Esta nueva regulación incluye a la legislación de nuestro país entre aquellas que de forma explícita establecen consecuencias penales, la respuesta más contundente del ordenamiento de cada Estado, al uso abusivo o manipulación de un sistema informático.

En la base de estas conductas de manipulación y abuso se encuentra indiscutiblemente un problema de seguridad de la información. Seguridad de la información en un triple aspecto: físico, lógico y jurídico. La seguridad física, quizá al ser la más palpable y cercana, es la que cuenta en nuestro país con un mayor grado de atención a nivel institucional y empresarial. Sin embargo el responsable de seguridad sabe que de la adecuada respuesta a las exigencias de la seguridad lógica del sistema de información depende, en buena medida, la propia subsistencia del mismo.

Los tres aspectos de la seguridad indicados (físico, lógico y jurídico) son complementarios y en modo alguno excluyentes entre sí. En este trabajo no se analizan todos los aspectos de la seguridad proporcionada a un sistema de información desde el ordenamiento jurídico español, sino que con detenimiento en la protección penal, otorgada por el nuevo Código, se analiza la respuesta de nuestro ordenamiento penal frente a conductas de fraude o manipulación informática. El efecto preventivo que la existencia de una amenaza penal

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

representa, la represión efectiva posterior a la comisión del hecho delictivo y el recurso al sector asegurador constituyen las principales medidas de seguridad jurídica implantadas en Derecho Español. Sin embargo la indemnización de la aseguradora, si es que se ha tenido la precaución de contratar un seguro, puede no ser una solución si se ha perdido la viabilidad de la propia empresa, organismo o institución. La implementación de medidas de seguridad a priori, preventivas, previas, se configura hoy como una necesidad más de todo sistema de información abierto al exterior. Es cada vez más habitual la utilización del sistema informático en una red de comunicación, la expansión en el uso de la red mundial Internet es una realidad incontestable. Los sistemas informáticos han dejado de ser una isla para convertirse en lugares de paso, de recepción y transmisión de información. Desde este planteamiento no puede descuidarse el control de acceso al sistema ni la información que sale de él. La integridad, confidencialidad, disponibilidad, autentificación y el no repudio del envío o recepción de un mensaje se han convertido en exigencias sin las cuales la indudable potencialidad comercial, económica, educativa que la comunicación de los sistemas informáticos otorga puede llegar a vaciarse de contenido. Por ello a lo largo del trabajo se recogen constantes alusiones a medidas de seguridad lógica que, implementadas previamente a la puesta en funcionamiento de cualquier sistema informático, prevengan y eviten conductas delictivas que aunque, bien es cierto, ya cuentan con respuesta desde el Código Penal y desde el sector asegurador a veces ésta no es la más eficaz. Porque creemos que ante la violación de un sistema de información la conclusión a la que se llega es que lo mejor es que nunca hubiera ocurrido.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

1. LOS ILÍCITOS INFORMÁTICOS

1.1. EL PROBLEMA DE LA INDIVIDUALIZACIÓN DE ESTAS CONDUCTAS.

1.2. EL PROBLEMA DE LA RECIENTE TIPIFICACIÓN DE ESTAS CONDUCTAS. (Referencia a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal).

1.3. CONCEPTO.

1.3.1. LA INFORMÁTICA COMO OBJETO DE LAS AGRESIONES Y COMO MEDIO PARA LA COMISIÓN DE ESTAS AGRESIONES.

1.3.2. LA INFORMÁTICA ÚNICAMENTE COMO MEDIO PARA LA COMISIÓN DE LAS CONDUCTAS ILÍCITAS.

1.3.3. TEORÍAS NEGATIVAS.

1.4. TIPOS.

1.4.1. AGRESIONES A LA ESFERA PRIVADA DEL CIUDADANO.

1.4.2. DAÑOS PATRIMONIALES OCASIONADOS POR LA MANIPULACIÓN ABUSIVA DE DATOS O PROGRAMAS DE PROCESAMIENTO AUTOMÁTICO.

1.5. ENCUADRAMIENTO DEL FRAUDE INFORMÁTICO DENTRO DEL ESQUEMA GENERAL DE LOS ILÍCITOS INFORMÁTICOS.

1.6. LA DIMENSIÓN INTERNACIONAL DE LOS ILÍCITOS INFORMÁTICOS Y DEL FRAUDE INFORMÁTICO EN PARTICULAR.

1.7. CONCLUSIONES

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

1. LOS ILÍCITOS INFORMÁTICOS

En una breve referencia histórica sobre el tema del delito informático se puede afirmar que todo el estudio sobre esta materia 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, a la que más adelante haremos referencia[1].

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

[1] No es éste el único documento que sobre criminalidad relacionada con la informática ha sido emitido en el plano internacional. Merecen también especial mención los siguientes: documento de la Secretaría de la OCDE sobre criminalidad en relación con los ordenadores de 15 de noviembre de 1984, 2ª versión de 30 de agosto de 1985 y versión final de 18 de abril de 1986. Documento de la Comisión sobre criminalidad en relación con los ordenadores de la OCDE de diciembre de 1984. La Comunidad Europea distribuyó un documento de fecha 10 de diciembre de 1987 sobre "los aspectos jurídicos del delito informático y seguridad de los ordenadores". La oficina Intergubernamental para la Informática (IBI) se ha ocupado del tema de la delincuencia informática publicando tres documentos: Doc. IBI-DR 06, Doc. IBI-DR 07 y el Doc. IBI-DR 08. La Cámara Internacional de Comercio (ICC) ha tratado estos temas en el documento: Doc. 373/76 Rev. de 1988. Por último la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en el informe del Secretario General denominado "Proyecto de guía jurídica sobre las transferencias electrónicas de fondos" (A/CN.9/250) recoge en el Add.4 una referencia expresa al fraude informático (publicación en el volumen XV:1984 del Anuario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional).

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

que utilicen esa vía 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[2].

Con estas reflexiones queremos introducir este estudio centrado sobre uno de los posibles flancos de ataque a la integridad patrimonial del individuo (de las personas físicas o jurídicas en general), 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 (física o jurídica), es en ésta segunda donde queda subsumida la figura del fraude informático. Es por esto que en ella centraremos el objeto de este estudio.

1.1. EL PROBLEMA DE LA INDIVIDUALIZACIÓN DE ESTAS CONDUCTAS

La criminalidad económica que actualmente tiene mayor transcendencia es aquélla que se apoya o se sirve de medios fraudulentos. El fraude con sus características propias, se ha adaptado a los avances tecnológicos y en concreto a los referentes a la informática. No obstante conviene desde un principio establecer una serie de precisiones que permitan encuadrar correctamente la categoría criminológica o delictual (ya se verá a cuál de ellas dos pertenece) de los ilícitos informáticos.

Antes de la entrada en vigor del nuevo Código Penal español era sostenible defender la dicotomía entre la categoría criminológica y delictual en relación con el conjunto de conductas a las que se hará referencia, diciendo que éstas podían encajar en la categoría de conductas criminógenas pero no eran en puridad

[2] 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.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

delitos. No eran delitos puesto que no estaban tipificadas como tal en la legislación penal. Por tanto era más correcto hablar de "delincuencia o criminalidad informática" como categoría exclusivamente criminológica en tanto no se tipificasen estas conductas en la ley penal. En definitiva cabía concluir que esas conductas eran factores criminógenos, de alto riesgo, que precisamente por la peligrosidad social que entrañaban exigían una regulación por la legislación penal como último instrumento de control social. Sin embargo el panorama ha cambiado radicalmente desde el 25 de mayo de 1996 en que entró en vigor el nuevo Código Penal español. Como más adelante se analizará, la tipificación penal de conductas relacionadas con las Tecnologías de la Información y las Comunicaciones (TIC) y, en concreto, fraudes y manipulaciones informáticas que causan perjuicio al patrimonio de un tercero son ya DELITO en DERECHO ESPAÑOL.

Miguel Bajo Fernández en un trabajo, publicado en la Revista ICADE titulado: "Los delitos patrimoniales y económicos en el Proyecto de Código Penal español"[3], habla de delitos patrimoniales cometidos a través de la informática. Sirve esta cita para introducir la polémica cuestión que a continuación reproducimos. ¿Por qué se puede hablar de delito informático, o de delincuencia informática como una categoría criminal 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?

Quizá, como apunta Tiedemann[4], se trata de proteger no tanto bienes jurídicos distintos de los ya protegidos, sino objetos concretos[5] ¿Pero siguiendo esta línea

[3] BAJO FERNÁNDEZ, Miguel. *Los delitos patrimoniales y económicos en el Proyecto de Código Penal español*. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales y del Instituto Universitario de Administración y Dirección de Empresas. N° 29. 1993. Págs. 213 y ss.

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

[5] Es decir puede existir una extensa legislación penal protectora del derecho de propiedad, como efectivamente así ocurre (Título XIII del Libro 2° del C. Penal de 1973 y Título XIII del Libro 2° del vigente Código Penal que ha abandonado la terminología de delitos contra la propiedad, fuertemente criticada por parte de la doctrina, acoge la expresión delitos contra el patrimonio y el orden socioeconómico) y sin embargo no ser adecuada para la protección específica de un objeto de propiedad singular como puede ser una línea de comunicación.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 trascender 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 entonces lo que permitirá hablar de esos nuevos delitos?

Para Nimmer[6] hay que partir de las propias, en cuanto específicas, características del sistema informático para de este modo encontrar la especificidad del delito informático.

Así señala Gutiérrez Francés[7] cinco aspectos especialmente vulnerables en el ámbito de la informática que pueden constituir otros tantos objetos de protección: la fase de entrada de datos, la programación, el procesamiento de datos, la salida

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

[7] GUTIÉRREZ FRANCÉS, Mª Luz. *Fraude informático y estafa. (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos)*. Ministerio de justicia. Secretaría General Técnica. Centro de Publicaciones. Madrid 1991. Pág.64.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de datos y la telecomunicación de datos. Estos cinco aspectos darán lugar, como más adelante se verá, a otros tantos criterios de clasificación de los ilícitos relacionados con la informática.

De esta amplia gama de conductas ¿cuáles constituirán el objeto de este estudio? Sólo aquéllas que por la finalidad que persiguen tienden a obtener un lucro ilícito.

Así pues, **del amplio campo de la delincuencia informática únicamente se pretende analizar el correspondiente al fraude cometido mediante sistemas informáticos.**

Los espectaculares avances de las tecnologías de la información, a los que casi diariamente se asiste, abren un nuevo y amplio abanico de posibilidades de comisión de delitos.

1.2. EL PROBLEMA DE LA RECIENTE TIPIFICACIÓN DE ESTAS CONDUCTAS. (Referencia a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal)

Antes de la reforma en nuestro Derecho Penal positivo, que regulaba la nueva realidad social de los ilícitos informáticos, sólo cabía utilizar estas expresiones[8] desde un punto de vista formal no material. Esta situación ha cambiado desde mayo de 1996. Con el fin de acercarnos al nuevo panorama legal, deben tenerse 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 directa o indirectamente con los sistemas informáticos. Haciendo un somero repaso a los intentos de modificación de nuestra legislación penal en materia de delincuencia informática encontramos cómo los textos de 1980 y 1983 no dedicaban especial atención al tema de la delincuencia por ordenador. 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 desconocía cualquier implicación o ataque que ésta pudiera infligir en la esfera

[8] Criminalidad informática y delincuencia informática.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

patrimonial del individuo.

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

Tipifican, 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 Bohemero en la conducta delictiva han de distinguirse tres elementos fundamentales: 1º 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[9] parece que muchos de estos delincuentes de "cuello blanco" se ven

[9] GONZÁLEZ RUS, Juan José. *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos*

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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. 2º 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. 3º 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.

Hasta la aprobación del nuevo Código Penal español ¿dónde se encontraba el obstáculo que impedía hablar con rigor de conductas delictivas? Evidentemente en la tipicidad. Las conductas englobadas dentro del concepto de criminalidad informática no ofrecía duda, eran antijurídicas, culpables, concurriendo en ellas las circunstancias objetivas de punibilidad, merecedoras de una pena, pero no existía tal pena puesto que no estaban tipificadas, no eran conductas típicas recogidas y reflejadas como tal en el Código Penal o en Legislación pen. especial.

La falta de tipicidad impedía hablar de delitos informáticos y dejaba inmersas estas acciones en la nebulosa de los indiferentes penales.
Sin embargo la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal modifica esta situación, como más adelante se verá. El nuevo artículo 248.2., del Código Penal, tipifica como delito de estafa tradicional el fraude informático.

Concretando ahora el sistema jurídico del delito en el derecho penal español, nuestro Código Penal establece en su artículo 10:

"Son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la Ley".[10]

---

informáticos. Revista de la Facultad de Derecho de la Universidad Complutense. N° 12. Monográfico sobre Informática y Derecho. Madrid. Septiembre 1986. Pág. 111.

[10] Nuestro anterior Código Penal, texto refundido publicado por

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 suponía un escollo insalvable era 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".[11]

Si únicamente lo definido en la ley es penalmente ilícito, 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[12] 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 debe, por tanto, atenderse a la naturaleza del bien jurídico lesionado para establecer la figura delictiva adecuada. A nuestro entender estas dos posturas no son excluyentes sino que pueden, 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 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.

Decreto 3096/1973, de 14 de septiembre, conforme a la Ley 44/1971, de 15 de noviembre establecía en su artículo 1° "son delitos o faltas las acciones u omisiones dolosas o culposas penadas por la Ley".

[11] CONDE-PUMPIDO FERREIRO, CÁNDIDO. Derecho Penal. Parte General. Editorial COLEX. Madrid. 1990. Pág.97.

[12] 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 n° 30, junio 1993. Página 9 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Otra alternativa que se podría proponer en estos temas, en la misma línea de solución, sería considerar como delitos informáticos en sí únicamente aquellas 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"[13]. Esta solución propuesta es una de las posibles vías de esclarecimiento del oscuro problema que hoy representa la represión penal de los ilícitos informáticos.

Pues bien, el nuevo Código Penal (C.P.) ha optado por atender a la naturaleza del bien jurídico lesionado, a través del medio informático, para establecer la figura delictiva adecuada para su represión. Como a continuación se verá el nuevo C.P. utiliza los tipos tradicionales de la estafa, robo, daños, protección de la intimidad ... para dar entrada a los ilícitos informáticos. Se configuran éstos, por tanto, como nuevos medios de ataque a bienes jurídicos ya conocidos. Sin embargo esta afirmación no puede hacerse de forma categórica dado que algunos tipos dejan traslucir la protección de un nuevo bien jurídico, la información tratada automáticamente, aunque sea a través de un tipo tradicional; a continuación se analizará, por ejemplo, el nuevo artículo 264.2 que tipifica el delito de daños sobre datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

- Así la **intimidad y el derecho a la propia imagen** son penalmente protegibles 1º cuando se encuentren en soporte o medio informático y, 2º frente a **ataques informáticos**, en los artículos 197 y 198 del nuevo C.P. En concreto, las conductas tipificadas resumidamente son éstas: apoderarse de mensajes de correo electrónico, interceptar telecomunicaciones, utilizar cualquier artificio técnico de grabación o reproducción de cualquier señal de comunicación;

[13] 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 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.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

apoderamiento, utilización o modificación de datos reservados de carácter personal registrados en ficheros o soportes informáticos, electrónicos o telemáticos; acceso no autorizado a ficheros informáticos que contengan datos personales; difusión, revelación o cesión a terceros de los datos o hechos descubiertos por los métodos a los que se ha hecho referencia. El artículo 198 recoge las conductas descritas pero realizadas por autoridad o funcionario público, que fuera de los casos permitidos por la ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, las lleve a efecto.

- El bien jurídico del **Patrimonio y el Orden Socioeconómico** queda protegido frente a los ataques informáticos en el Libro II, Título XIII, en los Capítulos II y VI, del nuevo Código Penal.

El Capítulo II, De los Robos, tipifica en los artículos 238 y 239 como **robo con fuerza en las cosas** el uso de tarjetas magnéticas o perforadas perdidas o substraídas a su dueño.

El nuevo Código establece responsabilidades penales por el uso por tercero de tarjeta robada o substraída. De acuerdo con la normativa comunitaria[14] cabe afirmar la exoneración de responsabilidad del titular de tarjeta substraída por los cargos realizados con posterioridad a la denuncia del hecho de la substracción y la limitación de su responsabilidad a 150 euros por las disposiciones anteriores a la denuncia. Pero si se concreta o determina la responsabilidad penal será el responsable penal el que, siguiendo las disposiciones del nuevo Código Penal en relación a la responsabilidad civil derivada de los delitos, deba reparar todos los daños y perjuicios causados.

El nuevo Código Penal establece en el art. 239, que a los efectos del presente artículo se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Analizando este precepto, (239 in fine) la utilización ilícita de tarjetas con banda

[14] Recomendación de la Comisión de 17 de noviembre de 1988, relativa a los Sistemas de Pago y en particular a las relaciones entre titulares y emisores de tarjetas. (88/590/CEE).
Código de Buena Conducta del Sector Bancario Europeo relativo a los Sistemas de Pago mediante Tarjeta, de 14 de noviembre de 1990.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

magnética, se subsume en el tipo de robo con fuerza en las cosas. Por tanto los hechos consistentes en la substracción de una tarjeta o la utilización de una tarjeta perdida por quien no es su titular, constituirán un delito de robo con fuerza en las cosas. La tipificación de estas conductas ya había sido propuesta por la doctrina y por la Fiscalía General del Estado.

Sin embargo este artículo para parte de la doctrina presenta algunos inconvenientes. La equiparación en este precepto del uso ilícito de las tarjetas de crédito o de débito con las tarjetas electromagnéticas en general produce un tratamiento equivalente de conductas totalmente distintas.
En el supuesto de sustracción y utilización de una tarjeta magnética ajena (por ejemplo: tarjetas para apertura de puertas en hoteles), el agente supera el obstáculo puesto por el dueño para la protección de su propiedad, utilizando la tarjeta como si de una llave falsa se tratara. Pero un supuesto totalmente distinto es aquél en el que el agente utilizando la tarjeta magnética y el número de identificación personal correspondiente accede a los fondos existentes en la cuenta corriente de un cliente de un banco u otra entidad de crédito. En este caso es el banco o la entidad en general, la que facilita la disposición patrimonial porque previamente se ha producido un engaño que ha conducido a una creencia errónea de que el usuario de la tarjeta era el verdadero titular. Este segundo caso encaja más dentro del tipo de las defraudaciones y sin embargo se le da un tratamiento equivalente al del robo con fuerza en las cosas, como si de esta modalidad delictiva se tratara.

Utilizando esta vía de razonamiento cabría defender que **el uso fraudulento por un tercero de las tarjetas de crédito o de débito legítimas substraídas a su titular debería ser castigado no a través del delito de robo con fuerza en las cosas, sino a través del delito de estafa**.

El Tribunal Supremo aplica el tipo del robo con fuerza en las cosas considerando como llave falsa la tarjeta substraída y teniendo en cuenta que la posibilidad de disposición de dinero en efectivo hace subsumibles estas conductas en los tipos de los delitos de apoderamiento. Sin embargo, como se ha dicho, la doctrina no es unánime en la calificación de esta conducta. Para un sector la conducta se encuadraría en el delito de robo y para otro sector doctrinal es preferible hablar en estos supuestos de delito de estafa puesto que existe un engaño por parte del usuario ilegítimo.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Mantenemos como más adecuada la tipificación como delito de robo con fuerza en las cosas, la utilización de tarjeta legítima por un tercero. En estas conductas aunque existe un engaño a la entidad depositaria de los fondos no cabe apreciar una manipulación de un proceso informático, elemento necesario para apreciar la existencia del delito de estafa. Es únicamente la utilización de esta tarjeta falsificada la que constituye una manipulación del "input", y por tanto una de las formas de defraudación o manipulación informática propias del delito de estafa, que consigue la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Hasta aquí la situación queda ordenada si se concreta la responsabilidad penal en uno o varios sujetos, éstos responderán civilmente de todos los daños y perjuicios que su actuación haya ocasionado. El problema surge cuando no se llega a determinar la responsabilidad penal, que indudablemente existe como ya hemos expuesto en la utilización ilegítima de tarjetas electrónicas. De la lectura de los contratos que unen a entidades y titulares de tarjetas deducimos la generalizada exoneración de responsabilidad del banco o entidad en toda disposición hecha por cajero en la que se haya hecho uso del número de identificación personal (NIP) del titular. Hemos visto cómo el Código Penal reconoce la posible existencia de manipulaciones informáticas que pueden dar lugar a una transferencia no consentida de activo patrimonial, es posible que una de esas manipulaciones consista en la obtención del NIP de una tarjeta haciendo recaer toda la responsabilidad de la operación precisamente SOBRE la víctima de la misma. En los contratos entre entidad y titular de la tarjeta se establece una presunción general de que toda transacción llevada a cabo con el uso del NIP es responsabilidad del titular de la tarjeta. Establecer con este rigor una presunción de este tipo supone por parte de las entidades suministrar un sistema de uso de cajeros automáticos totalmente fiable que en ningún caso deje un resquicio de duda o posibilidad de uso o apariencia de uso del NIP por otra persona que no sea su titular legítimo. La realidad es que ese método infalible de acreditación no ha llegado y sin embargo el usuario está soportando una sobrecarga o un *plus* de responsabilidad sobre las deficiencias de un sistema, el de cajeros automáticos, que no ha puesto en funcionamiento y del que es un mero usuario.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Garantizar que un sistema de pago con tarjeta es totalmente seguro, es decir, que no pueden producirse errores o manipulaciones, que una tarjeta no puede utilizarse nada mas que por su legítimo titular actualmente sería posible conforme al actual estado de la técnica. Ahora bien en un justo equilibrio de las obligaciones en las relaciones entre cliente y entidad si se descarga la responsabilidad en el usuario por transacciones efectuadas con el NIP, en justa reciprocidad, la entidad debería proporcionar una infraestructura de cajero absolutamente segura.

En definitiva cuando la negligencia por parte del cliente del banco no sea tan fácil de establecer debe tenerse en cuenta una circunstancia fundamental: que "es el banco el que diseña los procedimientos básicos de seguridad y autorización" en las transferencias electrónicas de fondos y el cliente el que los pone en práctica. Desde este planteamiento es adecuado adoptar unos criterios que permitan repartir la responsabilidad entre banco y cliente, ya que éste usa los sistemas que el banco pone a su alcance sin mediar negligencia por parte del cliente. Si el fraude se produce obedece a dos categorías de razones fundamentalmente: o bien ha existido una falta de diligencia por parte del cliente o bien **los procedimientos de seguridad y autorización establecidos por el banco eran inadecuados**. Pero en la mayoría de las ocasiones la determinación de si la orden fraudulenta responde a una o a otra de estas categorías no resulta fácil. Se debe tender a buscar fórmulas que sirvan para resolver la mayoría de los casos. En los contratos que ligan al cliente con su banco, la mayoría de ellos, facultan al banco para debitar en la cuenta del cliente cuando la operación se ha llevado a cabo mediante un terminal activado por una persona utilizando el número de identificación personal del cliente. Este régimen cesa cuando el cliente pone en conocimiento del banco que su número de identificación personal o su palabra de paso le han sido substraídas. Por tanto la responsabilidad del cliente cesa en el momento que adopta las medidas necesarias para evitar la transferencia fraudulenta, mientras el funcionamiento del sistema es "normal" el riesgo de la transferencia fraudulenta lo soporta el cliente. El problema es que la calificación de funcionamiento "normal" del sistema la hace la entidad a nuestro entender aventuradamente puesto que no tiene los medios técnicos que de forma irrefutable determinen que una transacción se ha hecho con un NIP y que ese NIP ha sido negligentemente custodiado por su titular.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

El Capítulo VI "**De las Defraudaciones**", Sección 1ª "**De las Estafas**" contiene un artículo el 248.2 que dispone:

"También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna ***manipulación informática o artificio*** *semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".*

Con este artículo queda tipificado como delito de estafa tradicional el "fraude informático[15]". Para ello se ha sustituido el término "engaño" propio del delito de estafa, por el de "manipulación", evitando así las críticas o dificultades que mostraba el tipo de la estafa para considerar producido el mismo sobre una máquina y no directamente sobre una persona. Esta "manipulación", como más adelante tendremos ocasión de analizar, se puede producir en el *input* o entrada de los datos, en el proceso de los mismos, o bien, en el *output* o salida. En cualquier caso, las conductas tipificadas en este párrafo 2º del artículo 248 presentarán cada vez con más frecuencia, con la generalización en el uso de la red Internet, el problema de la ley penal aplicable. Nos estamos refiriendo a las denominadas manipulaciones a distancia en las que el lugar de comisión de los hechos delictivos (manipulación) no coincide con el lugar donde se produce el resultado dañoso (transferencia fraudulenta).

El artículo 249 del Nuevo Código Penal fija una serie de pautas a las que tendrá que sujetarse el juzgador para la fijación de la pena en el delito de estafa. Así este art. 249 dispone que:

"Los reos de estafa serán castigados con la pena de prisión de seis meses a cuatro años, si la cuantía de lo defraudado excediere de cincuenta mil pesetas. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los MEDIOS empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción".

[15] Algunos autores prefieren utilizar los términos de "fraude a través de la informática" en vez de "fraude informático". Reservan la denominación de "fraude informático" para aquellas conductas de utilización irregular de software en beneficio propio o de un tercero incurriendo en una infracción de la vigente normativa sobre protección de programas de ordenador.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

El artículo termina con una referencia abierta con la expresión "y cuantas otras circunstancias", aunque la doctrina opina que la redacción del precepto obliga al Juez o Tribunal a motivar la pena que imponga.

Hemos destacado, en mayúsculas, el elemento que puede tomarse en orden a la graduación de la pena, los medios empleados en la comisión de la estafa, ya que entendemos que la estafa cometida a través de medios informáticos debe resultar afectada por este elemento de graduación.

Pero en la determinación de la pena aplicable a un supuesto delito de estafa cometida por medios informáticos no sólo, entendemos, debe tenerse en cuenta este artículo 249, sino también, el art. 250.1.7º que establece:

"250.1. El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:
(...)
7º Se cometa abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional".

La agravación que recoge este artículo 250 se establece en dos escalones:

- uno para el caso de que concurra una única circunstancia de agravación, como por ejemplo la del número 7º y,
- otro que recoge el mismo artículo 250.2. para el caso de que concurran juntamente las agravantes de los números 6º[16] ó 7º con la 1ª. En estos casos la pena a imponer será de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

Creemos que en las conductas de estafa informática podrá apreciarse en muchas ocasiones este segundo tramo en la agravación, ya que, si la estafa recae sobre sueldos, salarios, depósitos u otros activos de la víctima y, revistiendo especial

[16] Art. 250.1. " ....
1º Recaiga sobre cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social.
(...)
6º Revista especial gravedad, atendiendo al valor de la defraudación, a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

gravedad la defraudación, coloca a aquélla en una comprometida situación económica, la pena puede llegar a los ocho años de prisión y multa de hasta veinticuatro meses.

- Dentro del mismo Título XIII, por tanto dentro del ámbito de protección penal del mismo bien jurídico (Patrimonio y Orden Socioeconómico), el Capítulo IX "**De los Daños**" para aquellos que excedan de cincuenta mil pesetas, el artículo 264.2. dispone: *"La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos"*. La protección que otorga este artículo recae directamente sobre la información tratada de forma automática entendiendo que su destrucción lleva aparejados menoscabos importantes en el patrimonio de sus propietarios.

- El Capítulo XI, del ya citado Título XIII, bajo el título "**De los Delitos relativos a la Propiedad Intelectual e Industrial al Mercado y a los Consumidores**" recoge en el artículo 270 la protección penal al titular de derechos de propiedad intelectual sobre programas de ordenador[17]. Las penas

[17] Los derechos de propiedad intelectual sobre los programas de ordenador se reconocen en derecho español a través de tres vías: la civil, la administrativa y la penal. La vía de protección civil tiene su marco legislativo en el artículo 10 de la Ley 22/1987, de 11 de noviembre de la Propiedad Intelectual que expresamente establece "son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas y científicas, expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas (...) los programas de ordenador". Posteriormente la Ley 16/1993, de 23 de diciembre, ha incorporado al Derecho Español la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre protección jurídica de los programas de ordenador. Esta ley 16/93 ha adaptado la legislación española a la normativa comunitaria. Cabe destacar entre las medidas de protección, que recoge la citada Directiva, aquéllas que corresponde adoptar a los estados miembros contra los que pongan en circulación una copia de un programa de ordenador a sabiendas, o con posibilidad de saber, que se trata de una copia obtenida por procedimientos ilegítimos, o aquel que tenga con fines comerciales una copia de un programa de ordenador, presumiendo su carácter ilícito. Así mismo se considera necesario adoptar medidas contra la tenencia con fines comerciales de cualquier medio cuyo único propósito sea facilitar la supresión o neutralización de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador. Todas estas medidas han encontrado reflejo en la nueva tipificación que de los delitos contra la Propiedad Intelectual ha llevado a cabo el nuevo Código Penal.

La segunda vía de protección mencionada, la administrativa, está

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

previstas en este artículo son de prisión o multa. En el caso de la prisión oscila de seis meses a dos años, y en el caso de la multa de seis a veinticuatro meses. Como en el Código Penal anterior el nuevo C.P. castiga, con las penas transcritas, la copia no autorizada (piratería) de programas de ordenador (software). Esta protección penal deviene de la consideración por la Ley de Propiedad Intelectual, de 11-11-87 (22/87), a los programas de ordenador como objetos de por Propiedad Intelectual.

El artículo 270.1 exige para la aplicación del tipo el ánimo de lucro en el autor y el perjuicio de tercero. Sin embargo el párrafo segundo del mismo artículo 270 exige únicamente una acción intencionada (sin hablar de ánimo de lucro ni de perjuicio de tercero) de importación, exportación o almacenaje de las obras objeto de protección en el artículo. Con ello entendemos quedan comprendidas las conductas de los denominados "Hakers" que almacenan estas obras o producciones o ejecuciones sin autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. En estas conductas es indiferente la existencia o no de ánimo de lucro.
Como innovación frente a la regulación anterior ha de destacarse el párrafo final de este artículo 270 que dice:

"Será castigada también con la misma pena la fabricación, puesta en circulació y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador".

Este párrafo inserto en sede de protección penal de los derechos de propiedad intelectual sobre programas de ordenador hace pensar que la sanción se establece para aquellas conductas que neutralizando los sistemas lógicos de protección de un programa consiguen la copia del mismo y su posterior reproducción. Sin embargo, la dicción de este párrafo no circunscribe la conducta de neutralización a la finalidad de copia y reproducción, por lo que cabría sostener la penalización de aquellas otras conductas de neutralización de la protección lógica de programas

constituida por un conjunto de medidas de este carácter recogidas en la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) y por la adhesión de España a los Acuerdos de Shenguen.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

que dejen expedita o permitan la entrada en sistemas de información. Estamos considerando una serie de conductas en las que la finalidad del autor no sea copiar el programa cuyas medidas de seguridad lógicas han quedado neutralizadas, sino conseguir el acceso al sistema informático que precisamente el programa neutralizado impedía. La fabricación y puesta en circulación de medios destinados a facilitar la supresión de medidas de protección de programas de ordenador creemos puede tener un ámbito de aplicación mucho más amplio que el que quizá ante una primera lectura cabe deducir de este artículo 270 *in fine*.

Si en los hechos concurre junto a la conducta exigida en el tipo básico (por ejemplo, copia de un programa de ordenador con ánimo de lucro y en perjuicio de tercero), alguna de las circunstancias recogidas en el párrafo segundo y tercero del artículo 270 (almacenaje de diseños de páginas web de Internet, tenencia de un medio para desproteger un programa de ordenador) viene en aplicación el tipo agravado (artículo 271). En estos casos el Juez puede decretar el cierre temporal o definitivo de la industria o establecimiento del condenado.

En cuanto al régimen de la responsabilidad civil derivada de estos delitos se mantiene igual que en la regulación del anterior Código, remitiéndose a las disposiciones en la materia de la Ley de Propiedad Intelectual en relación con el cese de la actividad ilícita y la indemnización de los daños y perjuicios.
Asimismo el artículo 272.2 prevé, en el supuesto de sentencia condenatoria, que el Juez o Tribunal pueda decretar la publicación de la sentencia, a costa del infractor, en un periódico oficial. Cabría en este punto apuntar que quizá la publicación de la sentencia en un periódico de tirada nacional, u otros medios de difusión de más generalizado acceso, se avenga mejor con la finalidad de resarcimiento y defensa de los intereses del titular del derecho de autor vulnerado y, así mismo, sea una eficaz medida de publicidad de la efectividad en la aplicación de la norma penal.

- La Sección 3ª (**"De los delitos relativos al mercado y a los consumidores"**) del mismo Capítulo XI ("De los Delitos Relativos a la Propiedad Intelectual e Industrial al Mercado y a los Consumidores") recoge en el artículo 278 una referencia a documentos escritos o electrónicos y soportes informáticos y una remisión al apartado 1 del artículo 197, en el que se habla de mensajes de correo electrónico, manipulación de las telecomunicaciones..., como medios sobre los que puede recaer la comisión de un delito de espionaje industrial.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

- Dentro del Título XVIII "**De las Falsedades**" el Capítulo II, "De las **Falsedades Documentales**", en su Sección 1ª recoge un artículo, el 390, que castiga la falsificación de documentos debiendo considerarse incluido dentro del concepto de documento aquellos que se encuentren en soporte electrónico dada la claridad con la que el artículo 26, del mismo cuerpo legal, define lo que a los efectos del nuevo C.P. ha de considerarse por documento:
"Art. 26. A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

  No se encuentra precedente de este artículo en el anterior Código Penal, y dada la amplitud de su formulación es indudable que cabe considerar incluidos en el concepto de documento aquellos que se encuentren en soporte electrónico.

- Dentro del mismo Título XVIII, el Capítulo III, artículo 400 sanciona la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores (falsificación de moneda y efectos timbrados y falsedades documentales). La dicción del presente artículo es amplia aunque si se tiene en cuenta la restricción del concepto de moneda, artículo 387[18], las actuaciones delictivas en torno a lo que se denomina dinero electrónico[19] quedarían fuera del ámbito de aplicación de los tipos de

[18] Artículo 387: "... se entiende por moneda la metálica y papel moneda de curso legal. A los mismos efectos se considerarán moneda las tarjetas de crédito, las de débito y los cheques de viaje. Igualmente, se equipararán a la moneda nacional, la de la Unión Europea y las extranjeras".

[19] **Dinero electrónico** o "**E-Cash**" con estos términos se denomina al dinero virtual que es creado y utilizado dentro de una red abierta como puede ser Internet. El "E-Cash" sólo tiene valor dentro de la red. Este dinero electrónico se utiliza, por ejemplo, dentro de Internet para pagar por acceder a una base de datos, comprar un programa o cualquier otro bien o servicio ofertado dentro de la gran red. La funcionalidad del "E-Cash" muy simplificadamente es la siguiente: un usuario se conecta con Internet, se identifica como titular de una determinada cuenta y solicita de su banco o caja la retirada de dinero electrónico de su cuenta. La cantidad de dinero retirada se almacena como dinero digital en el disco duro del ordenador personal del usuario. A partir de aquí podríamos considerar la posibilidad de comisión de todos los delitos contra el patrimonio (robo, hurto, apropiación indebida ...) que tengan por objeto este dinero digital-electrónico. Como consecuencia de lo expuesto el usuario de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

falsificación de moneda y por tanto del ámbito del artículo 400.

- Por último el Título XXI, "Delitos contra la Constitución", del Libro II del nuevo C.P., recoge en su Sección 2ª "De los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad", en el artículo 536 el delito de violación de las telecomunicaciones por parte de una autoridad o funcionario, con infracción de las garantías constitucionales o legales, aunque medie causa por delito.
- En cuanto a las faltas cometidas por medio de o contra elementos informáticos comentaremos las cometidas contra el patrimonio. El nuevo Código Penal define las faltas en el artículo 13.3 como las infracciones que la ley castiga con pena leve. Centrándonos en las faltas contra el patrimonio el art. 623.4 establece que:

" Los que cometan estafa, apropiación indebida, o defraudación de electricidad, gas, agua u otro elemento, energía o fluido, o en equipos terminales de telecomunicación, en cuantía no superior a cincuenta mil pesetas".

Serán castigados con arresto de dos a seis fines de semana o multas de uno a dos meses.

Como consideraciones finales y sin perjuicio del análisis que más adelante se recoge, el nuevo marco penal definido por la Ley Orgánica 10/1995, de 23 de noviembre, no es la panacea que resuelve todos los ilícitos relacionados con el

---

Internet tiene dentro de la red su propio banco personal. Cuando el usuario quiere realizar un pago a través de la red debe confirmar su cuenta, el destino del pago y el importe. A continuación el software de dinero electrónico del usuario realizará una transferencia desde el disco duro al destino. El receptor-destino de la transferencia deposita el dinero digital que recibe en su propia cuenta. Las modalidades delictivas que cabe imaginar sobre la base de esta operativa son muchas. Aunque sin duda la restrictiva definición de moneda contenida en el artículo 387 del nuevo C.P. excluye del ámbito del delito de falsificación de moneda la alteración o incremento del dinero digital. Hoy son muchas las empresas que ofertan sus productos en Internet y permiten el pago a través de dinero electrónico. Estas operaciones ciertamente pueden no quedar reflejadas en la contabilidad de las empresas ni en el registro de exportaciones o importaciones. En definitiva la Hacienda española no tiene, al menos de momento, control de las transacciones realizadas vía Internet.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ordenador. Los ilícitos informáticos presentan unas características intrínsecas que dificultan sobremanera su persecución. Así podemos enumerar como características intrínsecas que dificultan la represión: la rapidez en su comisión, la facilidad para borrar las pruebas (no debe olvidarse que habitualmente el delincuente pertenece a la plantilla de la empresa), la facilidad para encubrir el hecho, la dificultad de la prueba sobre soporte magnético. Además de estas dificultades pertenecientes al orden de los hechos, las cuestiones de derecho que se suscitan tanto en el plano sustantivo como procesal, en aquellas conductas delictivas cometidas a distancia, plantean problemas de derecho internacional de a veces no fácil solución.

1.3. CONCEPTO

1.3.1. LA INFORMÁTICA COMO OBJETO DE LAS AGRESIONES Y COMO MEDIO PARA LA COMISIÓN DE ESTAS AGRESIONES

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 Romeo Casabona [20] 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. Como bien expone el citado autor, igual que los avances en el ámbito de la automoción fueron delimitados, regulados y reducidos a un ámbito criminógeno concreto, los nuevos avances en el

[20] ROMEO CASABONA, Carlos María. *Poder informático y seguridad jurídica*. Fundesco. Madrid 1987. Pág. 41.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

mundo de la informática y su potencial delictivo ha de ser identificado y regulado.

Pero en este primer acercamiento al tema de la criminalidad informática conviene hacer una clasificación general de estos hechos para de este modo centrar el tema principal de estudio: el fraude informático. Antes de pasar a la clasificación se dará un repaso a las distintas definiciones que sobre el fenómeno de la criminalidad informática se han propuesto por parte de la doctrina.

Para empezar, la criminalidad informática es un concepto amplio en el que no sólo se toma en cuenta a la informática como medio o instrumento para cometer un delito, sino también como objeto de la conducta ilícita. En este mismo sentido se manifiesta Gutiérrez Francés[21] al decir que la informática juega ante el Derecho Penal un doble papel: por un lado como objeto del delito y por otro lado como instrumento del comportamiento criminal.

La definición del fenómeno no es uniforme, así Tiedemann considera que la expresión "criminalidad mediante computadoras" alude a "todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos"[22]. Esta definición se puede calificar de omnicomprensiva ya que tanto hace referencia al problema de la agresión a la esfera de la intimidad del individuo, como por otra parte a los daños patrimoniales que se pueden producir por el uso abusivo o malintencionado de estos equipos automáticos de procesamiento de datos.

En esta misma línea, aunque con un mayor detalle en la delimitación de las conductas que pueden englobarse dentro de esa categoría de ilícitos informáticos patrimoniales, González Rus[23] habla de los "ilícitos

[21] GUTIÉRREZ FRANCÉS, Mª Luz. *La criminalidad defraudatoria por medios informáticos en el Anteproyecto de nuevo Código Penal de 1992.* III Congreso Iberoamericano de Informática y Derecho. U.N.E.D.- Mérida. 1992. Documentación existente en soporte magnético.

[22] TIEDEMANN, Klaus. *Poder económico y delito.* Ed. Ariel. Barcelona. 1985. Pág. 122.

[23] GONZÁLEZ RUS, Juan José. *Aproximación al tratamiento penal de los*

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

patrimoniales" polarizando estas conductas en torno a los siguientes puntos: " 1) Atentados y peligros para la intimidad que se derivan de la formación y explotación de bancos de datos personales. 2) Uso abusivo de los equipos e instalaciones informáticas y, en particular, el llamado <<hurto de tiempo>>,... 3) Introducción de datos o registros fraudulentos. 4) Alteración o destrucción de informaciones o ficheros. 5) Sustracción, divulgación de informaciones, ideas, proyectos, etc., contenidos en el ordenador. 6) Tutela del software. 7) Transferencias fraudulentas de dinero, instrumentos de crédito, propiedades, etc., mediante la manipulación del ordenador que interviene en la gestión de operaciones financieras, bancarias, etc. 8) Repercusión penal de la falsificación o alteración de los datos contenidos en el ordenador o de los informes generados por el mismo, especialmente en lo relativo a su consideración como documento y su validez probatoria. 9) Violación por parte de los encargados del proceso electrónico de datos, de la obligación específica del secreto informático". Continúa este autor con una serie de consideraciones criminológicas afirmando la incardinación de estas conductas entre las nuevas formas de criminalidad de cuello blanco. Y a su vez incluye esta criminalidad de cuello blanco[24] como forma de la criminalidad económica. Conviene llegados a este punto hacer alguna precisiones. Primero: consideramos, siguiendo así al profesor Bajo Fernández, que no son identificables los conceptos de delincuencia de cuello blanco y delincuencia económica. Segundo: la delincuencia económica en realidad es una especie de la de "cuello blanco". Tercero: de

ilícitos patrimoniales relacionados con medios o procedimientos informáticos. Revista de la Facultad de Derecho de la Universidad Complutense. N° 12. Monográfico sobre Informática y derecho. Madrid. Septiembre 1986.

[24] Entendemos la delincuencia de "cuello blanco" de acuerdo con la definición dada por Sutherland, es decir, como una "violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional". Por otro lado parece que el concepto generalmente aceptado de delincuencia económica es aquél que la conceptúa como la "relativa a las infracciones lesivas del orden económico cometidas por personas de alto nivel socio-económico en el desarrollo de su actividad profesional". De acuerdo con esto la mayoría de los autores que están de acuerdo en inscribir la criminalidad informática entre la delincuencia económica, lo están en inscribirla también entre la delincuencia de "cuello blanco" sin establecer los matices que distinguen una de otra categoría.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

acuerdo con las definiciones recogidas en la nota al pie última anterior, las dos definiciones que se recogen hablan del autor de la infracción como una persona con un "alto nivel socio-económico" y que la conducta la lleve a cabo en el desarrollo de su actividad profesional. Si se estudian con detenimiento las conductas concretas que se engloban en la categoría de la delincuencia informática muchas de ellas no reúnen estas dos características[25]. Por ello estimamos más adecuado considerar como una categoría criminológica independiente a la delincuencia informática.[26]

Por otra parte Romeo Casabona siguiendo la línea adoptada por los dos anteriores autores, entiende más acertado distinguir en el concepto de la criminalidad informática su doble vertiente delictiva: por una parte ataque a la intimidad personal y por otra lesión de intereses patrimoniales. En relación al primer ámbito de ataque hace algunas precisiones más, diciendo que no es únicamente la intimidad personal la que puede verse afectada sino también bienes supraindividuales "como son la fe pública, la seguridad nacional y tal vez la seguridad del flujo transnacional de datos".[27] De acuerdo con esto Romeo Casabona se encuentra cerca de un sector de la doctrina que distingue tres grupos dentro de la categoría de la

[25] La afirmación que sostenemos según la cual sólo en contadas ocasiones el autor pertenece a altas capas de la sociedad, viene corroborada por muchos otros autores en la doctrina española. Así Romeo Casabona habla que los autores "suelen ser primarios u ocasionales", empleados de las empresas víctimas de la delincuencia informática. Gutiérrez Francés al hablar del delincuente informático recoge las consideraciones de un estudio efectuado por el *National Center for Computer Crime* de acuerdo con las cuales los sucesos más graves en esta materia se han llevado a cabo por sujetos que trabajaban en el mundo de la informática, empleados en definitiva de las empresas afectadas. Se ha acuñado ya un término identificador de estos sujetos los "insiders", es decir los que están dentro del sistema que vulneran. Por su parte Tiedemann habla de personas de inteligencia y clase media que acuden a estos métodos delictivos esporádicamente. Se trata de autores casuales, sin grandes conocimientos técnicos en informática. Señala así mismo este autor que no debe olvidarse el nuevo tipo criminológico de los jóvenes estudiantes que con fines, en muchas ocasiones, exclusivamente de autoafirmación personal penetran en grandes sistemas informáticos manipulando datos y programas.

[26] ALASTUEY DOBON, M.C. *Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial.* III Congreso Iberoamericano de Informática y Derecho. U.N.E.D.- Mérida. 1992. s.p.

[27] ROMEO CASABONA, C.M. Op. cit. Pág. 42.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

criminalidad por computadora: el grupo de los delitos contra la propiedad, el de los delitos contra los derechos de la personalidad y un tercer y último grupo de delitos contra bienes jurídicos supraindividuales o sociales[28]. Por tanto descarta este autor definiciones parciales del fenómeno de la delincuencia informática que como la de Parker restringe el concepto al ámbito de lo estrictamente patrimonial. De acuerdo con su visión general de la delincuencia informática define ésta en su esencia, dejando para ulteriores precisiones el ámbito al que afecta (el patrimonio o la intimidad). Así define la delincuencia informática como "un aspecto de la criminalidad caracterizado por una nueva dimensión que explica su especificidad, ambas notas las aporta el ordenador junto con sus funciones propias más importantes: el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines. Cualquier conducta que no opere sobre la base de estas funciones, aunque pueda resultar delictiva, no poseerá ya esa especificidad y deberá ser, por tanto, apartada del estudio de la delincuencia vinculada a la informática o tecnologías de la información"[29].

En esta misma línea amplia en la conceptuación de la criminalidad informática se inscribe la Profª. Corcoy [30], al entender que esta criminalidad no puede ser adecuadamente comprendida sino se estudian todas sus posibles implicaciones tanto en el campo de la "esfera privada del ciudadano" como en su esfera patrimonial.

Por otra parte Sieber [31] no se detiene en las consideraciones que establecen la distinción entre criminalidad informática y delito informático y utiliza ambas expresiones de forma alterna a lo largo de todo su estudio. Sí le

---

[28] Vid. en este sentido Sieber, *Informationstechnologie* ..., p. 14; Winkelbauer, *Computerkriminalität*..., p.40; Lenckner, *Computerkriminalität*..., p. 15 y ss.

[29] ROMEO CASABONA, C.M. Op. cit. Pág. 43.

[30] CORCOY, M. *Delitos contra el patrimonio cometidos por medios informáticos*. Revista Jurídica de Cataluña. Nº 3. Barcelona 1988. Págs. 133 y ss.

[31] SIEBER, Ulrich. *Criminalidad informática: peligro y prevención*. En vol. "Delincuencia informática". S. Mir Puig (comp.). Ed. PPU. Colección IURA-7. Barcelona. 1992. Págs. 29 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

preocupa a este autor determinar las características de los delitos cometidos a través del ordenador que hacen de estas actuaciones delictivas nuevas formas de criminalidad distintas de los clásicos delitos contra la propiedad. Apunta como tales características: la permanencia y automatismo del hecho, sumas de daños, dificultades de averiguación y rápido crecimiento de este tipo de delitos. Para este autor, exponentes suficientes, para individualizar estas conductas como un tipo "sui generis" de criminalidad.

Siguiendo con este repaso de la doctrina científica en relación con la delimitación conceptual de la criminalidad informática conviene recoger la opinión de Gutiérrez Francés, que partiendo del reconocimiento de la extrema dificultad para situar los límites del fenómeno criminal relacionado con la informática, admite la expresión "criminalidad informática ... como categoría exclusivamente criminológica y de carácter funcional"[32].

Gutiérrez Francés prefiere como método de acercamiento al fenómeno de la criminalidad informática aquél que parte de las propias características del sistema informático, para desde ellas desentrañar las consecuencias dañosas que en los distintos ámbitos de la personalidad pueden tener su uso malintencionado. Se invierte en este caso el método de estudio de estas conductas, no partimos de las consecuencias,[33] sino que llegamos a ellas a través del análisis de las causas.

La especificidad de la delincuencia informática la aporta, por tanto, el ordenador con sus funciones básicas: el procesamiento y la transmisión de datos y la ejecución de programas para tales fines. Con esto se eliminan del ámbito de la delincuencia informática todas aquellas conductas que no operen sobre la base de alguna de las funciones vistas. Una conducta delictiva aunque se encuentre vinculada con las nuevas tecnologías de la

[32] GUTIÉRREZ FRANCÉS, Mª Luz. *Fraude informático y estafa. (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos)*. Ministerio de Justicia. Centro de publicaciones. Secretaría General Técnica. Madrid. 1991. Págs. 62 y ss.

[33] Agresiones a la esfera privada del ciudadano y daños patrimoniales ocasionados por la manipulación abusiva de datos o programas de procesamiento automático.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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.

Por último _ Davara Rodríguez adelantándose en su momento a una realidad que hoy ya vivimos, la tipificación en la legislación penal de estas conductas como delitos informáticos, adopta la terminología de delito informático, prescindiendo por tanto del concepto más genérico de criminalidad informática, y lo 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*"[34]. 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 vistas en teorías anteriores.

1.3.2. LA INFORMÁTICA ÚNICAMENTE COMO MEDIO PARA LA COMISIÓN DE LAS CONDUCTAS ILÍCITAS.

Aldama Baquedano[35] expone una amplia casuística donde la informática aparece como medio para la comisión de conductas delictivas. El medio informático "por la entidad propia" que desarrolla en la realización de la conducta delictiva puede convertirse en el núcleo de la conducta y configurar un delito en sí, en este caso un delito informático. Por tanto para esta autora el conjunto de conductas denominadas delitos informáticos vienen configuradas desde la utilización de medios informáticos en su comisión. La importancia que el medio informático presente en el total de la conducta ilícita, es la que determinará que se pueda hablar o no de delito informático.

---

[34] DAVARA RODRÍGUEZ, Miguel Ángel. *Derecho Informático*. Ed. Aranzadi. Pamplona. 1993. Pág.318.

[35] 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.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Entender que la informática únicamente, en el campo del derecho penal, juega el papel de medio para la comisión de conductas ilícitas es una visión parcial del fenómeno de la delincuencia informática y, en nuestra opinión, por parcial una visón inacertada. Ahora bien considerar la informática como medio para la comisión de ilícitos permite introducir el siguiente punto dedicado a los criterios de clasificación de estas conductas. A través de los medios informáticos puede agredirse al patrimonio, a la intimidad o a ambos bienes, de una persona. Pero quedan fuera todas aquellas agresiones donde la informática, o bien, un nuevo bien jurídico como es la información sobre la información[36] se ven agredidos.

1.3.3. TEORÍAS NEGATIVAS

No conviene cerrar esta cuestión sin hacer referencia a aquella parte de la doctrina que niega la posibilidad de atribuir a la criminalidad por computadora un contenido específico. Para estos autores la especificidad del fenómeno informático implicada en estas conductas no crea una nueva forma de criminalidad, ni configura nuevas categorías de delitos[37].

1.4. TIPOS

1.4.1. AGRESIONES A LA ESFERA PRIVADA DEL CIUDADANO

Todas las clasificaciones de los ilícitos informáticos que a continuación se recogen pueden afectar a dos bienes jurídicos distintos: el patrimonio o la intimidad del individuo. Estas clasificaciones, por tanto, atienden a criterios formales, que posteriormente son llenados por el bien jurídico al cual afectan.

Se desarrolla con mayor amplitud el apartado correspondiente a los

[36] BUENO ARUS, Francisco. *El Delito Informático*. Revista Actualidad Informática Aranzadi. N° 11. Abril 1994. Página 2.

[37] En este sentido confrontar con autores como: HAFT, *Das Zweite esetz...*, p.6 y SIEG *JURA*, 1986, p. 352.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ataques al patrimonio al encontrarse el fraude informático dentro de este sector.

La **intimidad** puede ser agredida a través de la utilización de medios informáticos y de ello tuvo ya conciencia el legislador constitucional español al establecer en el artículo 18.4 de la Carta Magna que

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

La intimidad se configura así, como un derecho fundamental con una protección reforzada ante los Tribunales establecida por la propia Constitución, por la Ley de *Protección Jurisdiccional de los Derechos Fundamentales de la Persona*, de 26 de diciembre de 1978, y por la Ley Orgánica de 5 de mayo de 1982 *sobre Protección del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*. Junto a estas leyes el mandato constitucional, del artículo 18.4 aludido, se cumple con la aprobación de la Ley Orgánica de *Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, (LORTAD)* de 29 de octubre de 1992. Si esta es la protección de que goza la intimidad[38] en derecho español en el ámbito extrapenal, en el penal la protección era reducida, casi inexistente, antes de la promulgación del Nuevo Código Penal. Autorizada doctrina, entre otros el Prof. Bueno Arús[39], afirmaba en interpretación de las disposiciones de nuestro anterior Código Penal que, los ataques a la intimidad producidos a través de medios informáticos no encontraban entrada en los tipos penales vigentes salvo en el 497 bis que sancionaba al que para descubrir los secretos o la intimidad de otros sin su

[38] Se entiende por *intimidad* aquellos datos de una persona que, "unidos al individuo, se pueden considerar como características que definen a la persona y a su entorno, en su convivencia social". Pero el derecho no solo protege la intimidad sino algo más, la *privacidad*. Bajo este término de privacidad se alude al conjunto de noticias sobre una persona que pueden configurar su perfil o su trayectoria humana, y que esta persona tiene derecho a mantener en su esfera interna. Cfr. DAVARA RODRÍGUEZ, M.A. *Derecho Informático*. Editorial Aranzadi. Pamplona. 1993. Página 56.

[39] BUENO ARUS, Francisco. *El Delito Informático*. Revista Actualidad Informática Aranzadi. N° 11. Abril 1994. Página 1 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

consentimiento, intercepta sus comunicaciones telefónicas. Si esta manipulación de las comunicaciones telefónicas se realiza en una operación en la que haya intervenido un ordenador se estaría ante un supuesto de agresión a la intimidad por medios informáticos. El artículo 192 bis contemplaba una conducta similar a la expuesta, pero era en ese caso cometida por autoridad, funcionario público o agente de éstos.

Una regulación más específica de los ataques informáticos a la intimidad se recogía en el *Proyecto de Ley Orgánica del Código Penal* de 1992.

Los delitos contra la intimidad y el secreto de las comunicaciones venían regulados en el artículo 198.2 haciéndose en este artículo una referencia expresa a la informática al decir: "las mismas penas se impondrán al que, sin estar autorizado, se apoderase de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o cualquier otro tipo de archivo o registro público o privado". Se producía una agravación de la pena si los datos descubiertos se difundieren o revelaren a terceros. Si los hechos que describía el tipo se llevaban a cabo "por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros... y si difundieren o revelaren los datos reservados" la pena llegaba hasta cinco años de prisión.

El Anteproyecto de Ley Orgánica de Código Penal recogía en el libro II, título IX los delitos contra la intimidad y el domicilio. El capítulo I, de dicho título, se dedicaba a los delitos de descubrimiento y revelación de secretos. El artículo 188 recogía en el apartado 2 una formulación idéntica a la del artículo 198.2 del Proyecto del 92. Las diferencias venían de las penas a imponer en el caso de difusión o revelación a terceros de los datos reservados descubiertos. En estos casos el Anteproyecto del 94 elevaba las penas, de uno a tres años que establecía el Proyecto del 92, a privación de libertad de dos a cinco años. En cuanto a los encargados o responsables de los ficheros, soportes informáticos, archivos o registros, que realicen estos hechos, la pena será de prisión de tres a cinco años. Pero si divulgaren o revelaren los datos reservados la pena podía llegar hasta seis años.

Si estos son, resumidamente, los antecedentes del nuevo Código Penal

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(aprobado por Ley Orgánica 10/1995, de 23 de noviembre) la **protección de la intimidad frente a los ataques de la informática** queda recogida en el **vigente artículo 197 del C.P.**:

"197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, MENSAJES DE CORREO ELECTRÓNICO o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las ***penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.***

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, DATOS RESERVADOS DE CARÁCTER PERSONAL O FAMILIAR DE OTRO QUE SE HALLEN REGISTRADOS EN FICHEROS O SOPORTES INFORMÁTICOS, ELECTRÓNICOS O TELEMÁTICOS, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la ***pena de prisión de dos a cinco años*** *si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

Será castigado con las ***penas de prisión de uno a tres años y multa de doce a veinticuatro meses****, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.*

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá ***la pena de prisión de tres a cinco años****, y si se difunden, ceden o revelan los datos reservados, se impondrá* ***la pena en su mitad superior.***

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

El Nuevo Código utiliza el sistema de días-multa consistente en la imposición al condenado de una sanción pecuniaria. De acuerdo con el artículo 50, del actual Código Penal, la cuota diaria tendrá un mínimo de doscientas pesetas y un máximo de cincuenta mil. A efectos de cómputo, cuando se fije la duración por meses o por años, se entenderá que los meses son de treinta días y los años de trescientos sesenta. Son los Jueces y Tribunales los que determinarán, motivadamente, en cada caso la extensión de la pena de multa.

El vigente artículo 197 tipifica como acciones básicas:

1º. El apoderamiento de papeles o cartas, mensajes de correo electrónico, la interceptación de la correspondencia o la utilización de artificios, con el fin de descubrir los secretos y vulnerar la intimidad de otro. En este tipo básico, el soporte electrónico de datos concernientes a la intimidad de los individuos está clara y plenamente incluido como objeto de protección. Expresamente el Código habla de "mensajes de correo electrónico" y de interceptar las telecomunicaciones. Es evidente que el medio (informático o electrónico), no puede convertirse en un obstáculo para la protección de la intimidad del individuo. La protección penal que el Código otorga en este tipo básico ha de entenderse abarca a las personas físicas y jurídicas dado que el artículo 200 del vigente Código Penal dice: *"Lo dispuesto en este Capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código".*

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Esta remisión a otros preceptos del Código ha de entenderse referida a los artículos 277, 278, 279 y 285 que juegan como normas especiales al tipificar los delitos relativos a la Propiedad Intelectual e Industrial, al mercado y a los consumidores. El descubrimiento, revelación o cesión de datos reservados de personas jurídicas (se encuentren o no en soportes informáticos) relativos a los temas indicados será castigado por los citados artículos que operan como norma especial.

2°. Apoderarse, utilizar o modificar datos reservados de carácter personal que se encuentren en ficheros o soportes informáticos, electrónicos o telemáticos. El apartado 2 del artículo 197, que venimos analizando, no destaca, ciertamente, por su claridad ya que junto a las conductas señaladas penaliza el acceso, alteración y utilización en perjuicio del titular de los datos o de un tercero de éstos que se encuentren almacenados en ficheros o soportes informáticos. Decimos que no destaca por su claridad ya que primero penaliza el apoderamiento, utilización y modificación de datos en perjuicio de tercero, sin mencionar el perjuicio al propio titular de los datos, y después recoge una conducta similar de alteración y utilización ahora ya sí incluyendo en perjuicio del titular o de un tercero.

Por otra parte, resulta también complicado el juego de las agravaciones. Estas se pueden clasificar en los siguientes grupos:

- por razón de las personas que llevan a cabo la conducta delictiva: personas encargadas o responsables de los ficheros, archivos o registros; si el sujeto agente es autoridad o funcionario público (art. 198).

- Por el carácter de los datos objeto de la agresión si revelan la ideología, religión, creencias, salud, origen racial o vida sexual.

- Por la condición del titular de los datos: menor o incapaz.

- Por el ánimo de lucro del agente.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

1.4.2. DAÑOS PATRIMONIALES OCASIONADOS POR LA MANIPULACIÓN ABUSIVA DE DATOS O PROGRAMAS DE PROCESAMIENTO AUTOMÁTICO.

Pasando ya al estudio más detallado de las propuestas de ordenación de los ilícitos informáticos se puede apreciar su extrema variedad e incluso oposición en algunos casos. Las propuestas de clasificación recogidas han de entenderse dirigidas a agredir el patrimonio personal o colectivo de los individuos. Bajo el epígrafe "las diversas formas delictivas y su prevención" aborda este tema Ulrich Sieber[40]. Sieber comienza hablando de un primer grupo de conductas, las denominadas manipulaciones del ordenador consistentes en la modificación de datos, no especificando de momento, si se trata de datos de entrada, en el proceso o bien datos de salida, que permite obtener un enriquecimiento personal al autor de dicha modificación. La casuística es muy amplia y no merece la pena detenerse aquí en ella. Lo que quizá sí merezca la pena es estudiar el método a través del cual se llevan a cabo estas conductas. Este autor considera el ordenador como una instalación para el proceso de datos y de la forma particular de trabajo de la máquina deduce los diferentes flancos de ataque o manipulación. El criterio clasificador adoptado es aquél que partiendo de las funciones básicas que desarrolla un sistema de ordenador, analiza las manipulaciones que en cada fase pueden sufrir los datos manejados por el sistema. Esta primera clasificación es especialmente interesante para nuestro objeto de estudio ya que a su vez parte de la consideración de que estas conductas se llevan a cabo con ánimo de obtener un enriquecimiento personal. No es ésta una clasificación omnicomprensiva de todas las conductas englobables dentro del ámbito de los ilícitos informáticos, pero sí es adecuada para adentrarnos en el estudio de las conductas fraudulentas relacionadas con el uso de sistemas informáticos.

Las manipulaciones pueden afectar al "input", al programa , a la consola, al "output" y, por último, producir abusos en el denominado tiempo

[40] SIEBER, Ulrich. *Criminalidad informática: peligro y prevención*. En vol. "Delincuencia informática". Santiago Mir Puig (Comp.). Barcelona 1992. Pág. 15 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

compartido y en los sistemas de teleproceso.

Las manipulaciones del "input" consisten en la modificación de los datos de entrada en el ordenador, de forma que aunque su posterior proceso sea el habitual se produce un resultado falso. La mayoría de las manipulaciones de sistemas informáticos descubiertas hasta ahora se han producido en esta fase. Los autores son empleados de las propias entidades o empresas afectadas encargados de la organización y comprobación de los datos de entrada en el proceso.

Las manipulaciones del programa requieren un mayor grado de especialización técnica por parte del autor al llevarse a cabo una modificación en las instrucciones del programa. Aquí los datos de entrada permanecen inalterados, pero el tratamiento al que se les somete es falseado produciéndose por ello resultados también falsos. Son estas conductas mucho más difíciles de detectar, al programar la máquina para que borre automáticamente los rastros de la manipulación del programa una vez efectuada ésta.

Las manipulaciones de la consola pertenecen a aquel grupo de manipulaciones que se llevan a cabo incidiendo de forma ilícita sobre los elementos físicos del sistema o de la instalación. Un caso especial dentro de estas manipulaciones del servicio mecánico de la instalación son las manipulaciones de la consola. Una operación aparentemente tan sencilla como puede ser el mal uso de la tecla de interrupción puede convertirse en el origen de la falsificación de todo un proceso.[41]

[41] Un ejemplo de una de estas manipulaciones es recogido por Sieber en su artículo "Criminalidad informática: peligro y prevención", publicado en el volumen *Delincuencia Informática*, S. Mir Puig (Comp.), PPU, Barcelona 1992, páginas 20 y ss. El caso se produjo en la República Federal de Alemania a mediados de los años setenta en el Banco de Herstatt. Con manipulaciones de la consola se ocultaban negocios de especulación de divisas del Banco de Herstatt. El sistema adoptado por el banco para registrar las operaciones en el mercado de divisas era el siguiente: las cantidades totales del comercio de divisas y dinero del banco se registraban con el teclado de un mini-ordenador y posteriormente se transferían al ordenador central del banco. Para ocultar algunos negocios de especulación de divisas los empleados implicados pulsaban la tecla de interrupción de la consola del mini-ordenador evitando transferir la información sobre la conclusión de la operación especulativa al ordenador central del banco y por tanto evitando su conocimiento por la dirección.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En cuanto a las manipulaciones del "output" se produce una modificación de los datos de salida, es decir, el resultado de un procesamiento. Esta manipulación puede producirse cuando los datos se plasman en un soporte papel, en la pantalla de un ordenador o en un soporte magnético.

Por último este autor hace referencia dentro de esta primera categoría de conductas englobables en la delincuencia informática, a los abusos cometidos a través del sistema de trabajo en tiempo compartido. Muchas de las manipulaciones anteriormente vistas pueden llevarse a cabo por empleados de las empresas perjudicadas, pero también pueden cometerse por otros usuarios que haciendo uso, valga la redundancia, del sistema en tiempo compartido con los empleados tienen las mismas posibilidades de manipulación que éstos. Tampoco debe olvidarse a aquéllos que acceden al sistema a través de una red de comunicaciones.

Junto a estas conductas de manipulación, que serán las que se desarrollen en el siguiente capítulo por ser dentro de ellas donde encuentra acomodo el fraude informático, Sieber recoge otras categorías de delincuencia informática como son: el espionaje informático y hurto de software, el sabotaje informático, el hurto de tiempo y la utilización del ordenador para la comisión de delitos económicos en general. A nuestro juicio las conductas recogidas en esta última categoría pueden ser incluidas dentro de la primera serie de manipulaciones del sistema informático. Así por ejemplo el caso recogido por Sieber dentro de esta última categoría es claramente un modo de manipulación del "input". Recoge este autor las estafas de la Equity-Funding-Corporation una compañía de seguros que vendió contratos de seguros de vida ficticios a unos reaseguradores. Es evidente que esta estafa se encuentra de lleno dentro del ámbito de la delincuencia económica y se vio muy favorecida su comisión por el uso de los medios informáticos, pero también parece indiscutible su clasificación como una forma de manipulación del "input" de un sistema informático. Las distintas formas de manipulación de un sistema informático pueden convertirse en las nuevas formas de comisión de los delitos económicos. Por tanto sostenemos la eliminación de este último criterio de clasificación y su inclusión dentro del primero.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Siguiendo con el repaso a los criterios de clasificación dados por la doctrina en relación con la criminalidad informática haremos referencia a los utilizados por Romeo Casabona[42].

Los criterios de clasificación como pone de manifiesto el autor son muy variados. Recoge una clasificación meramente descriptiva dada por Brown[43] en la que distingue hasta seis categorías de delitos: "la interferencia física en las instalaciones del ordenador o en partes de él, la extracción o copia de los datos contenidos en un sistema informático, la alteración o deformación de los datos contenidos en un sistema informático, la utilización del ordenador como instrumento real o simbólico para la comisión de otros tipos delictivos, la utilización de tiempo del ordenador y la interferencia en la comunicación entre instalaciones".[44]

A continuación se recoge una clasificación basada en la figura del fraude informático en la que Jaeger adoptando un criterio clasificativo paralelo al de Sieber habla del fraude relativo a la materia corporal del ordenador (sabotaje informático), el fraude a nivel del input, a nivel del tratamiento y a nivel del output. La adopción de la terminología común de fraude para designar a todas estas conductas exige o bien una interpretación amplia de concepto de fraude o por el contrario entender esta clasificación con un carácter parcial. El repaso de éstas y otras clasificaciones del fenómeno de la criminalidad relacionada con la informática lleva a concluir a Romeo Casabona que los dos elementos fundamentales que permitirán posteriormente agrupar correctamente las conductas delictivas relacionadas con el ordenador son aquéllos que distinguen entre la consideración de la informática como instrumento o medio comisivo y la informática como objeto de la agresión. Sin embargo ante esta aparente sencillez en la adopción de los criterios de clasificación Romeo Casabona descubre un foco de problemas en relación con la clasificación de aquellas conductas que suponen una agresión de bienes inmateriales. Por ejemplo la obtención

[42] ROMEO CASABONA, Carlos María. Op. cit. Página 43 y ss.

[43] BROWN, R.A. *Crime and computers*, en "Criminal Law Journal2, vol. 7,70 (1983).

[44] Romeo Casabona. Op. cit. Pág. 43 y 44.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

o destrucción de datos o de programas de un ordenador, que no suponen siempre una alteración o pérdida de los datos o de los programas pero que pueden ocasionar importantes perjuicios económicos al propietario. Las dificultades son grandes en el descubrimiento de todas las conductas que pueden afectar a los elementos lógicos del sistema. Estos elementos pueden ser atacados sin ser destruidos o manipulados simplemente al ser consultados por aquéllos que no tienen autorización. No olvidemos que los datos al convertirse en información para un determinado sujeto que los aplica a un fin determinado, pueden tener un valor económico muy superior a cualquier otro bien material.

En este mismo sentido se pronuncia González Rus[45] al clasificar los ilícitos patrimoniales relacionados con medios o procedimientos informáticos distinguiendo entre: delitos contra el sistema informático y delitos cometidos por medio del sistema informático. En los delitos contra el sistema informático éste resulta ser el objeto directo del ataque. Estas conductas en ocasiones encuentran fácil acomodo en las figuras delictivas tradicionales (robo, hurto, daños, etc.) y otras veces por la peculiaridad de la misma conducta se ven huérfanas de regulación (hurto de tiempo de uso de un ordenador, consulta no autorizada de datos, etc).

Como subcriterio de clasificación dentro del general de conductas contra el sistema informático, el autor apunta la distinción entre conductas que agreden a los elementos físicos del sistema y conductas que agreden a los elementos lógicos.

El segundo grupo fundamental de conductas lo constituyen aquéllas que utilizan los sistemas informáticos como medios comisivos. El sistema se convierte en el instrumento de la acción delictiva. Dentro de esta categoría general de delitos González Rus distingue: aquellos "delitos para cuya realización se utiliza el sistema informático a través de muy diversas manipulaciones del soporte lógico o mediante la utilización delictiva de los datos y programas", y aquellos otros delitos cuya comisión únicamente es posible con la intervención de medios informáticos, o bien son exclusivos

[45] GONZÁLEZ RUS, J.J. Op.Cit. Pág. 116 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

del medio informático.

Tiedemann ofrece un panorama general de la delincuencia surgida alrededor de la informática refiriendo algunos de sus aspectos que cara al exterior ofrecen una más fácil y clara constatación: un crecimiento de la automatización de los procesos contables a la vez que un aumento de las actuaciones delictivas en estos procesos, la posición del sector bancario como uno de los principales objetivos de ataque en la delincuencia informática, la falta de medidas de seguridad, la existencia de una alta cifra de conductas delictivas desconocida, bien por su falta de denuncia, bien por el absoluto desconocimiento de su comisión.

Una vez expuestas estas precisiones previas Tiedemann clasifica los hechos económicos punibles cometidos con el empleo de sistemas informáticos en cuatro grupos: manipulaciones, espionaje, sabotaje y hurto de tiempo.

Las manipulaciones, coincidiendo con la doctrina de otros autores, pueden afectar a la fase de suministro o alimentación (input) de datos, a la fase de salida (output) y a la fase de procesamiento. También pueden producirse manipulaciones en el hardware. Los sistemas de tratamiento de datos a distancia (teletratamiento) posibilitan cualquiera de las tres formas de manipulación de los datos antes expuestas.

El Prof. Davara[46] propone una ordenación del tema partiendo de considerar como criterios delimitadores de la categoría de los delitos informáticos, el medio y el fin. El medio de comisión, por tanto será un elemento, bien, o servicio patrimonial del ámbito de responsabilidad de la informática, y el fin que se persiga debe ser la producción de un beneficio al sujeto, autor del ilícito. A su vez el fin perseguido por el sujeto, autor, ha de causar un perjuicio a otro.

En un intento de clasificación de estas conductas englobadas bajo la denominación común de ilícitos informáticos se puede observar, como así

[46] DAVARA RODRÍGUEZ, M.A. *Derecho Informático*. Ed. Aranzadi. Pamplona 1993. Pág. 315 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

propone el Prof. Davara, dos conductas ilícitas que aglutinan al resto: el acceso y manipulación de los datos y, por otro lado, la manipulación de programas.

Así podemos hablar de:

"1) Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos.

2) Acceso a los datos y utilización de los mismos por quien no está autorizado para ello.

3) Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas.

4) Utilización del ordenador y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.

5) Utilización del ordenador con fines fraudulentos.

6) Agresión a la "privacidad" "[47].

1.5. ENCUADRAMIENTO DEL FRAUDE INFORMÁTICO DENTRO DEL ESQUEMA GENERAL DE LOS ILÍCITOS INFORMÁTICOS.

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. 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

[47]DAVARA RODRÍGUEZ, M.A. Op. cit. Pág. 323.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 explicaba al no existir como tal tipo penal en la legislación positiva (hoy con la promulgación del nuevo Código Penal el artículo 248.2 configura como delito de estafa tradicional el fraude informático) y la segunda al constatar la amplia gama de conductas que podemos situar dentro del fraude informático (estafa informática, falsedades por medios informáticos). Así mismo 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) [48]. Pero si la terminología de "fraude informático" no es pacífica no nos encontramos con criterios unificados en la denominación de la categoría más amplia de la criminalidad informática o el llamado "delito informático".

Siguiendo con la tarea de delimitación de nuestro ámbito de interés seguiremos a Agustín Domínguez[49] para determinar las características fundamentales del fraude informático: 1ª impacto financiero, 2ª queda involucrado el proceso electrónico de fondos en la perpetración o en el encubrimiento, 3ª 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 informática integrado por usos indebidos o manipulaciones fraudulentas de elementos informáticos de cualquier tipo que posibilitan un beneficio ilícito.[50] Este autor sistematiza las notas características del fraude

[48]GUTIÉRREZ FRANCÉS, Mª LUZ. *Fraude informático y estafa*. Ministerio de Justicia. Secretaría General Técnica. Centro de Publicaciones. Madrid. 1991. Pág. 89.

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

[50]CAMACHO LOSA, L. *El delito informático*. Madrid. 1987. pp. 25-26.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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.
Una vez expuestas las notas características básicas del fraude informático continuamos el análisis distinguiendo en estos delitos entre el medio y el fin. Se sigue así el método de análisis que para las figuras delictivas relacionadas con los medios informáticos propone el Prof. Davara .

Comenzando por el medio utilizado para la comisión del fraude debe ser " un elemento, bien, o servicio, patrimonial del ámbito de responsabilidad de la informática" y en cuanto al fin perseguido no ha de ser otro sino "la producción de un beneficio al sujeto o autor del ilícito" [51].

Como pone de manifiesto el Prof. Davara se puede observar cómo el conjunto de la criminalidad informática gira en torno a dos conductas ilícitas: el acceso y la manipulación de datos o bien la manipulación de programas. Pues bien ambas conductas ilícitas pueden constituir fraude electrónico si se realizan mediando las características propias del fraude electrónico.

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.[52]

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.

---

[51] DAVARA RODRÍGUEZ, M.A. Op. cit. Pág. 320.

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

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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.

2. Manipulaciones en el programa.

   La entrada de datos es correcta pero una manipulación del 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 medidas se adoptan 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 las 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. Hoy la

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

extensión creciente en el uso de la red mundial Internet, pone en la primera línea de análisis los problemas jurídicos derivados del cada vez mayor número de actos y contratos realizados en y a través de la gran red. En una red global como Internet la multitud de individuos e instituciones que confluyen hace inevitable que algunos quieran acceder a lugar a los que no tienen autorización (hackers) o quieran destruir datos o sistemas una vez violado su acceso (crackers). En el amplio mundo de la Red, y con ánimo simplificador, podemos decir que los ataques más frecuentes pueden dirigirse al usuario final o bien a la seguridad de los sistemas corporativos. El usuario final puede sufrir usurpación de sus datos (más adelante veremos los posibles problemas que plantea el envío de números de tarjetas de crédito por la red), alteración de la integridad de la información enviada o bien suplantación de la personalidad bien sea del usuario final o del servidor con el que el usuario conecta y le da acceso a la Red. Veremos como el recurso a sistemas de seguridad criptográficos asimétricos es la solución más idónea para garantizar privacidad, autentificación de usuarios, integridad y no repudio en las comunicaciones en Internet. En cuanto a los ataques a sistemas corporativos en Internet el principio básico que sustenta el diseño de seguridad en la mayoría de estos sistemas es mantener a los intrusos fuera para poder trabajar dentro de la red. Con ello se establecen los denominados "FireWall" o cortafuegos[53].

Con las manipulaciones a distancia 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,

[53] En una red de ordenadores un cortafuegos es un dispositivo que protege a una red privada de los accesos públicos. El cortafuegos tiene una doble función: por una parte bloquea el tráfico proviniente de direcciones no autorizadas o accesos a zonas restringidas y, por otra parte, permite el flujo de operaciones autorizadas. Un cortafuegos debe atender como objetivos prioritarios a: impedir usurpaciones de identidad e integridad de la información; permitir el acceso a las direcciones de origen válidas y autorizadas; filtrado de solicitudes de conexión desde la red interior al exterior; protección de los datos de identidad de los usuarios autorizados; protección frente a determinadas formas de delitos informáticos como los denominados "caballos de troya". Ahora bien de nada servirá un "FireWall" sin un adecuado diseño conjunto de seguridad en la institución. V. *Las Tecnologías de la Información en la Empresa*. Cuadernos de CINCO DÍAS. Nº 9 Internet. "La red".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

geográficamente distantes, y son múltiples las conexiones entre sistemas informáticos de diferentes Estados.

1.6. LA DIMENSIÓN INTERNACIONAL DE LOS ILÍCITOS INFORMÁTICOS Y DEL FRAUDE INFORMÁTICO EN PARTICULAR

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 aunque escaso un reciente tratamiento en el ámbito de derecho penal 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[54] donde plantea fundamentalmente la siguiente cuestión: la determinación del lugar de la comisión de una manipulación de datos o de 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

[54] VILARIÑO PINTOS, Eduardo. *El delito informático. Derecho comparado y aspectos jurídico-internacionales.* En vol. *Hacia un Nuevo Orden Internacional y Europeo.* Editorial TECNOS. Pág.807 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 delincuencia informática internacional.

Por último y para asegurar un más alto grado de 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 la misma flexibilidad y facilidad que para la comisión de los hechos delictivos proporcionan los sistemas telemáticos.

CONCLUSIONES

De las distintas concepciones y clasificaciones que sobre el fenómeno de la delincuencia informática se han expuesto algunas consideraciones deben ser destacadas.

Primero: la informática, o mejor dicho, su uso ilícito puede representar una grave amenaza tanto para el patrimonio o intereses patrimoniales del individuo como para su intimidad.

Segundo: la informática en estos ataques, al patrimonio o a la intimidad, puede ser medio o instrumento en la comisión de la acción delictiva o bien el objeto de la agresión que repercute posteriormente en el patrimonio de un individuo, o en su intimidad[55] .

[55] Por ejemplo el espionaje de datos contenidos en soporte informático cuya divulgación afecte a la intimidad del titular de esos datos.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Tercero: de las conductas descritas sólo centraremos el posterior estudio en aquéllas que tengan su repercusión en la esfera patrimonial del individuo, ya se cometan utilizando la informática como instrumento o como objeto de la agresión.

Cuarto: Aunque no sea objeto de estudio detallado en este trabajo, sí es destacable la cuestión referente al sistema de incriminación que se adopte para otorgar una respuesta penal a estas conductas. Los ilícitos informáticos que ya se había establecido *de lege ferenda* su carácter de conductas penalizables, por su alto contenido antisocial y por las graves consecuencias perjudiciales que pueden producir, hoy aunque de forma difusa, *de lege data* han quedado configuradas como delito, es decir, como conductas antijurídicas, típicas, culpables y punibles. Decimos que de forma difusa dado que 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 con una dificultad dogmática considerable y con un resultado, al menos en apariencia, deslavazado. Se valora muy positivamente la tipificación, en el nuevo Código Penal, de conductas en que se utilizan los medios informáticos o telemáticos para la comisión de delitos contra el patrimonio o contra la intimidad. Así mismo algunos otros preceptos protegen derechos o bienes directamente relacionados con el tratamiento automatizado de la información, intervengan o no en el proceso las telecomunicaciones.

Pese a la tipificación hecha por el nuevo Código Penal no nos resistimos a apuntar una forma alternativa de incriminación. De acuerdo con esta forma habría un delito informático en el que el bien jurídico protegido fuera la información tratada automáticamente en cualquiera de sus tres estados: almacenada, en proceso y en tránsito. Y como aspectos a proteger, de esa información, habría de atenderse a las características propias de la misma, es decir, integridad, privacidad, autoría y punto de emisión. Junto a este delito una pléyade de delitos tradicionales con la referencia *cometido por medios informáticos*, sería una solución alternativa. [56]

[56] 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.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

2. CONCEPTO DE FRAUDE INFORMÁTICO

2.1. CONCEPTO EN LA LEGISLACIÓN INTERNA: CÓDIGO PENAL publicado por Decreto 3096/1973, de 14 de septiembre, PROYECTO DE LEY ORGÁNICA DEL CÓDIGO PENAL (121/000102) DE 1992, ANTEPROYECTO DE LEY ORGÁNICA DE CÓDIGO PENAL DE 20 DE MAYO DE 1994 Y NUEVO CÓDIGO PENAL aprobado por L.O. 10/1995, de 23 de noviembre.

2.2. CONCEPTO EN LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO ESPAÑOL. (Referencia a jurisprudencia menor en relación con el uso abusivo de medios de pago).

2.3. CONCEPTO EN LA NORMATIVA SUPRANACIONAL

2.3.1. PROYECTO DE GUÍA JURÍDICA SOBRE LAS TRANSFERENCIAS ELECTRÓNICAS DE FONDOS: INFORME DEL SECRETARIO GENERAL DE LA CNUDMI

2.3.2. RECOMENDACIÓN DEL CONSEJO DE EUROPA R(89)9 SOBRE CRIMINALIDAD INFORMÁTICA

2.4. EL BIEN JURÍDICO PROTEGIDO EN EL FRAUDE INFORMÁTICO

2.5. ELEMENTOS BÁSICOS DEL TIPO:

2.5.1. ANIMO DE LUCRO

2.5.2. ENGAÑO

2.5.3. DOLO. INTENCIÓN DE MANIPULAR REGISTROS INFORMÁTICOS

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

2.5.4. PERJUICIO PATRIMONIAL PARA LA VICTIMA

2.5.5. INFORMÁTICA COMO MEDIO PARA LA COMISIÓN DEL FRAUDE

2.6. ELEMENTOS PERSONALES CAUSALES: SUJETO AGENTE

2.7. ELEMENTOS VULNERABLES: OBJETO DE LA AGRESIÓN

2.8. ELEMENTOS DE RESULTADO: EFECTOS

2.8.1. PERJUICIOS PATRIMONIALES

2.8.2. AGRESIONES A LA IMAGEN DE ENTIDADES FINANCIERAS

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

2. CONCEPTO DE FRAUDE INFORMÁTICO

2.1. CONCEPTO EN LA LEGISLACIÓN INTERNA: CÓDIGO PENAL publicado por Decreto 3096/1973, de 14 de septiembre, PROYECTO DE LEY ORGÁNICA DEL CÓDIGO PENAL (121/000102) DE 1992, ANTEPROYECTO DE LEY ORGÁNICA DE CÓDIGO PENAL DE 20 DE MAYO DE 1994 Y NUEVO CÓDIGO PENAL aprobado por L.O. 10/1995, de 23 de noviembre.

En la determinación del concepto de fraude informático es obligada la referencia a la doctrina y a la casuística en general, pero no menos interesante es recoger la hasta ahora, salvo la nueva redacción dada al delito de estafa por el Código Penal de 1995, escasa legislación penal en la materia[57].

El repaso de los artículos del derogado Código Penal, publicado por Decreto 3096/1973, descubría la inexistencia de figuras típicas y la necesidad del recurso a las tradicionales formas de defraudación para encontrar una cobertura penal del fraude informático. No queriendo entrar, de momento, en el estudio de la adecuación de las figuras delictivas tradicionales para castigar las nuevas conductas de defraudación informática, sí analizaremos la tipificación expresa de estas conductas, de defraudaciones patrimoniales por medios informáticos, recogida en el Anteproyecto de Nuevo Código Penal de 1992, en el Proyecto de Ley Orgánica del Código Penal [58], en el Anteproyecto de Ley Orgánica de Código Penal de 1994 y en el Nuevo Código Penal aprobado por L.O. 10/1995.

El Anteproyecto del 92 destina a las defraudaciones patrimoniales por medios informáticos dos preceptos:

- el artículo 238 *in fine* establece que a los efectos del presente artículo (delito

[57] Antes de la entrada en vigor del nuevo Código Penal no sólo era escasa sino conflictiva. Así lo ponía de manifiesto Anguiano al decir que "en el actual Código Penal en lo que se refiere a estafa plantea un problema muy grave si se utiliza la informática como herramienta para delinquir". La nueva redacción del delito de estafa (art. 248.2) permite ampliar a estas conductas la incriminación penal. Cfr. ANGUIANO, J.M. *El asesoramiento es la mejor solución actual para las compañías que quieren salvaguardar sus recursos informáticos.* Revista Seguridad Informática, nº 8, diciembre 1993. Año II. Página 52 y ss.

[58] Publicado en el Boletín Oficial de las Cortes Generales de 23 de Septiembre de 1992, serie A. Núm. 102-1.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de robo) se consideran llaves falsas las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

- El segundo precepto es el 248.2 en el que se tipifica la estafa mediante ordenador. Dice este precepto que también cometen estafa los que, con ánimo de lucro, realizan una manipulación informática que interfiera el resultado de un procesamiento o transmisión informática de datos y así ocasionen un perjuicio a otro.

Analizando el primer precepto, (238 *in fine*) la utilización ilícita de tarjetas con banda magnética, se podrá subsumir en el tipo de robo con fuerza en las cosas. Por tanto el robo de una tarjeta o la utilización de una tarjeta perdida por quien no es su titular, constituirá robo con fuerza en las cosas. La tipificación de estas conductas ya había sido propuesta por la doctrina y por la Fiscalía General del Estado.

Sin embargo este precepto para parte de la doctrina, entre los que se encuentran autores como Gutiérrez Francés o De la Mata presenta algunos inconvenientes. La equiparación en este artículo del uso ilícito de las tarjetas de crédito o de débito con las tarjetas electromagnéticas en general produce un tratamiento equivalente de conductas totalmente distintas. En el supuesto de sustracción y utilización de una tarjeta magnética ajena (por ejemplo la tarjeta de apertura de puerta en hoteles), el agente supera el obstáculo puesto por el dueño para la protección de su propiedad, utilizando la tarjeta como si de una llave falsa se tratara. Pero un supuesto totalmente distinto es aquél en el que el agente utilizando la tarjeta magnética y el número identificador (PIN *Personal Identification Number*) correspondiente accede a los fondos existentes en la cuenta corriente de un cliente en un banco. En este caso es el banco el que facilita la disposición patrimonial porque previamente se ha producido un engaño que ha conducido a una creencia errónea de que el usuario de la tarjeta era el verdadero titular. Este segundo caso encaja más dentro del tipo de las defraudaciones y sin embargo se le da un tratamiento equivalente al del robo con fuerza en las cosas, como si de esta modalidad delictiva se tratara. En el punto 2.2. analizaremos cómo la jurisprudencia menor (de Audiencias Provinciales) ha conocido ya de supuestos de uso fraudulento de tarjeta robada o extraviada por tercero. Estas causas son ventiladas en la vía civil dada la casi total imposibilidad de identificación del delincuente que llevó a cabo los hechos. El reparto de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

responsabilidades, por tanto, se efectúa entre entidad emisora y titular de tarjeta.

Estos supuestos de uso de tarjeta por tercero no autorizado son analizados por el Prof. Ruiz Vadillo[59] al tratar el uso fraudulento de las tarjetas magnéticas o tarjetas perforadas que permiten el acceso a la habitación de muchos hoteles u otros recintos. La falsificación de estas tarjetas hace que nos encontremos ante una llave falsa.

Por tanto el uso fraudulento de las tarjetas de crédito o de débito debe merecer, a nuestro entender, una reprobación penal independiente a la establecida para el robo con fuerza en las cosas[60].

Resumiendo, **las tarjetas electrónicas utilizadas para la obtención de efectivo de los denominados cajeros automáticos pueden dar lugar a muy diversas situaciones penalizables con arreglo a distintos tipos pero sólo una de esas utilizaciones, creemos, entraña las características propias del fraude informático**. La tarjeta electrónica puede ser la tarjeta legítima o por el contrario una tarjeta falsificada. **Es la utilización de esta tarjeta falsificada la que constituye una manipulación del "input", y por tanto una de las formas de fraude informático**[61].

---

[59] RUIZ VADILLO, Enrique. *"Algunas consideraciones sobre la delincuencia informática"*. Actas de las Jornadas sobre Abogacía e Informática 7 y 8 de mayo de 1993. Ilustre Colegio de Abogados de Barcelona. Barcelona. 1993. Pág. 112 y ss.

[60] La conducta que se viene analizando de manipulación de cajeros automáticos para la obtención ilícita de una suma de dinero no tiene una calificación jurídica uniforme en la doctrina, ni coincide con la interpretación dada por la Jurisprudencia. El Tribunal Supremo aplica el tipo del robo con fuerza en las cosas considerando como llave falsa la tarjeta substraída y teniendo en cuenta que la posibilidad de disposición de dinero en efectivo hace subsumibles estas conductas en los tipos de los delitos de apoderamiento. Sin embargo, como se ha dicho, la doctrina no es unánime en la calificación de esta conducta. Para Romeo Casabona la conducta se encuadraría en el delito de hurto de acuerdo con la cantidad substraída. Para otro sector doctrinal es preferible hablar en estos supuestos de delito de estafa puesto que existe un engaño por parte del usuario ilegítimo.

[61] En opinión del Prof. Bueno Arús estas conductas deberían calificarse jurídicamente como un concurso entre falsedad de documento y estafa. Cfr. BUENO ARUS, Francisco. *El Delito Informático*. Actualidad Informática Aranzadi. N° 11, abril de 1994. Pág. 1 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En cuanto al segundo precepto, antes comentado, de la estafa informática del artículo 248.2 del Anteproyecto, recoge con mayor aproximación las conductas a las que nos referiremos en este capítulo dedicado al fraude informático. Cuando se habla de fraude informático esta denominación no tiene una correspondencia con una figura tipificada penalmente de forma independiente[62] pero sin embargo, a nuestro juicio, es defendible su reconocimiento como delito independiente al proteger un bien jurídico nuevo: la no manipulación del tratamiento automatizado de la información, se encuentre ésta ya almacenada en soporte electrónico, en proceso o en tránsito. Ese tipo independiente de fraude informático no debería circunscribir el ámbito subjetivo de ataque a los intereses individuales de un tercero sino a todos los posibles afectados representados por los intereses difusos de los consumidores, la seguridad en el tráfico mercantil, etc...

Retomando el análisis del Anteproyecto de 1992 lo primero que el citado documento lleva a cabo es una simplificación de las conductas englobables dentro del fraude informático o de las defraudaciones por medios informáticos, dejando reducidas éstas a las defraudaciones exclusivamente patrimoniales.

Esta figura también ha recibido algunas críticas por parte de autores como Gutiérrez Francés al entender que se trata de una tipificación del fraude informático excesivamente simplista, que atiende exclusivamente a intereses patrimoniales individuales. Es decir, con esta tipificación se están dejando fuera todas aquellas manipulaciones fraudulentas de elementos informáticos que afecten, por ejemplo, al sistema de cotizaciones bursátiles, a los intereses de accionistas y consumidores en general, etc. Con estos antecedentes ya cabía predecir que el fraude informático se incorporaría en la actual legislación penal utilizando como hilo conductor el tipo de la estafa con todas las limitaciones que ello conlleva, como así lo ha puesto de manifiesto la Jurisprudencia del Tribunal Supremo. De este modo el tipo propuesto en el artículo 248.2 del Anteproyecto sólo servirá para reprimir un grupo reducido de conductas del amplio marco de las

[62] Decimos que no hay un tipo penal independiente de fraude informático porque el Nuevo Código Penal en el artículo 248.2 dice que "*También se consideran reos de ESTAFA los que, con ánimo de lucro, y VALIÉNDOSE de ALGUNA MANIPULACIÓN INFORMÁTICA o artificio semejante consigan la TRANSFERENCIA NO CONSENTIDA de cualquier ACTIVO PATRIMONIAL en perjuicio de tercero*". Por tanto lo que sin duda son unas conductas calificables como "fraude informático" el vigente Código Penal las penaliza a través del tipo tradicional de la estafa, no se crea un tipo independiente de FRAUDE INFORMÁTICO.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

defraudaciones mediante computadora. Se atiende a la lesión de bienes patrimoniales individuales y se olvidan las lesiones a bienes supraindividuales como los antes apuntados. Aparte de otro problema fundamental en el tipo de la estafa cual es el del engaño. Si el engaño es elemento fundamental en la estafa es realmente difícil apreciar su concurrencia en el caso de engaño a una máquina[63]. Más adelante se abordará con mayor detenimiento este tema en el análisis de las declaraciones jurisprudenciales del Tribunal Supremo.

En cuanto al **Proyecto de Ley Orgánica del Código Penal de 1992**[64] es amplia la regulación de los denominados delitos informáticos, en comparación con textos legales anteriores. Recoge una serie de preceptos que tipifican las siguientes conductas: ataques a la intimidad y al secreto de las comunicaciones provenientes de la informática, la infracción de los derechos de propiedad intelectual de los programas de ordenador, dentro de los delitos relativos a la propiedad industrial al mercado y a los consumidores se recoge la protección penal de las topografías de los productos semiconductores y en el Capítulo VI del Título XII la Sección 1ª trata bajo el título "de las defraudaciones" de los ilícitos informáticos de carácter patrimonial. Parece que el Proyecto del 92 opta por la figura de la estafa para lograr la represión de los ilícitos patrimoniales informáticos. Así dice este texto legal, "también cometen estafa los que, con ánimo de lucro, realizaren una manipulación informática que interfiera el resultado de un procesamiento o transmisión informática de datos, y así ocasionaren un perjuicio a otro".

Recoge este artículo los elementos fundamentales del fraude informático que servirán para delimitar estas conductas y excluir todas aquellas otras que siendo ilícitos informáticos no pueden calificarse de fraude informático. Estos elementos se resumen en tres fundamentales: ánimo de lucro del autor, manipulación informática y perjuicio patrimonial para tercero. La manipulación informática exige una alteración del normal funcionamiento del sistema informático bien en

[63] El Nuevo Código Penal resuelve el problema sustituyendo el término "engaño", incluido en el tipo de estafa tradicional, por el de "manipulación". Cfr. Artículo 248.2 del Código Penal texto aprobado por Ley Orgánica 10/1995, de 23 de noviembre.

[64] Proyecto de Ley Orgánica del Código Penal (121/000102) publicado en el Boletín Oficial de las Cortes Generales, Congreso de los Diputados, Serie A: Proyectos de Ley, Número 102-1, de 23 de septiembre de 1992.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

sus elementos físicos o lógicos[65].

El Anteproyecto de Ley Orgánica de Código Penal de 20 de mayo de 1994 recoge en su articulado diversos preceptos que bien de una forma directa o bien indirectamente aluden a la utilización de medios informáticos en la comisión de los ilícitos penales. La exposición se centrará, a continuación, en la tipificación del delito de **estafa** y en el **robo con fuerza en las cosas**, al ser estos dos tipos penales los que mejor se ajustan a la **represión de las conductas de fraude informático** que se vienen examinando.

El Capítulo II "de los robos" del Título XII "delitos contra el patrimonio y contra el orden socioeconómico", tipifica el **robo con fuerza en las cosas** en el artículo 230 y en el siguiente artículo especifica qué ha de entenderse por **llave falsa** incluyendo dentro del concepto de llave "**las tarjetas, magnéticas** o perforadas, y los mandos o instrumentos de apertura a distancia". Con esto el Anteproyecto del 94 no se aleja de lo ya establecido en el Proyecto del 92. Pero no recoge una regulación exhaustiva de las conductas delictivas relacionadas con la utilización de las tarjetas electrónicas. Como ya se vio anteriormente el uso de la tarjeta electrónica dará lugar a uno u otro delito dependiendo del carácter de ésta, legítima o falsificada[66] y, en el caso de la tarjeta legítima, del modo como se haya substraído a su titular o si es el mismo titular el que la utiliza del tipo de infracción contractual que cometa. Toda esta amplia y variada casuística no es abordada en el Anteproyecto del 94 debiendo remitirnos de nuevo a la interpretación de la doctrina y de la Jurisprudencia para encontrar la respuesta

[65] Recoge el Proyecto del 92 otra serie de referencias indirectas a la utilización de medios informáticos en delitos tradicionales por ejemplo: en los robos con fuerza en las cosas la utilización de tarjetas magnéticas como llaves falsas, en los delitos de estragos se establece "los que causaren estragos por medio de... perturbación grave de cualquier clase o medio de comunicación" quedando incluidos, como no, los medios telemáticos de transmisión de datos, en los delitos de falsedades documentales "se considera documento todo papel o soporte material que exprese o incorpore datos, hechos o narraciones de inmediata o potencial relevancia jurídica o eficacia probatoria", en el delito de infidelidad en la custodia de documentos y de la violación de secretos se hace referencia a elementos documentales en una clara referencia amplia de este concepto. Cfr. *La Informática en la Legislación*. Actualidad Informática Aranzadi. Abril de 1994 número 11. Sección Legislación. Página 1 y ss.

[66] La tarjeta legítima robo o hurto, y la falsificada estafa, por manipulación del *input*.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

jurídica que se ofrece a estas conductas, sin lugar a dudas, delictivas.

El mismo **Título XII**, antes aludido, recoge en su **Capítulo VI "de las defraudaciones"**, en la **Sección Primera "de las estafas"**, en el artículo 241, la **estafa cometida a través de la realización de alguna manipulación informática**.

Dice el punto 2 del artículo 241: "*también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*".

Recoge esta modalidad de estafa todas las características del fraude informático ya expuestas. Es el tipo de la estafa el elegido por el legislador para la represión de estas conductas. La crítica que, quizá, cabría hacer a esta regulación es la falta de adecuación del tipo de la estafa con las características de estas conductas. Por tanto no tiene mucho fundamento jurídico mantener una tipificación donde el elemento del engaño, columna vertebral de la estafa, es difícil de apreciar en las conductas de fraude informático. En la formulación de la estafa informática recogida en el Anteproyecto del 94 el elemento del engaño, aunque no de una forma explícita pero sí implícitamente, se recoge con la expresión "valiéndose de alguna manipulación informática". Por tanto es necesario acudir a una interpretación que explicite un elemento que en sí es esencial en la estafa y que, por tanto, debería estar explícito en una forma de estafa como han catalogado a la estafa informática[67].
Como en el Proyecto del 92, aquí también en este Anteproyecto de 1994, se castiga la infracción de derechos de propiedad intelectual de programas de ordenador en el artículo 248.

Es digno de un estudio independiente el artículo 254 que tipifica un delito de **uso**

[67] Agustín Domínguez resume así las principales características del fraude informático: "acto intencionado de manipulación y alteración de registros con ánimo de lucro", a lo que se añade un correlativo perjuicio para la víctima. Tampoco recoge este autor como elemento esencial en el fraude informático el engaño. Cfr. DOMÍNGUEZ, Agustín. *Transferencia Electrónica de Fondos y de Datos. Protección jurídica de los datos personales emitidos en una operación de pago electrónico*. En vol. Encuentros sobre Informática y Derecho 1992-1993. Coor. M.A. DAVARA. Aranzadi. Pamplona. 1993. Página 119 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de un terminal de telecomunicación subrepticiamente ocasionando un perjuicio al titular. Se encuentra este precepto dentro de una sección dedicada a las defraudaciones de fluido eléctrico y análogas. En esta sección, se castigan aquellas conductas que tienden a la utilización de algún tipo de energía o de servicios de telecomunicaciones sin respetar las normas que para su normal funcionamiento se han establecido. Se está pensando por tanto en la utilización de un terminal de telecomunicación sin contar, por ejemplo, con número de abonado, etc. Pero este artículo 254 admite, a nuestro juicio, una interpretación más avanzada. Cabría argumentar, no sin importantes dificultades dada la ubicación de este precepto, que el 254 protege al titular de un terminal de telecomunicación (un ordenador personal) con el que se ha cometido una acción o una operación de fraude informático a distancia. Un terminal de telecomunicación bien puede ser un ordenador personal (un PC doméstico) que conectado a la red telefónica transmita una serie de órdenes de transferencia de fondos (o por ejemplo órdenes de pago de compras realizadas vía Internet) que produzcan al titular de ese terminal un grave perjuicio económico. El legislador, desde el punto interpretativo en el que nos encontramos, habría dejado recaer el peso de toda la responsabilidad penal sobre aquél que de forma subrepticia ha utilizado el terminal. Se entremezclaría en este precepto una cuestión largamente debatida en relación con la pregunta de si ¿puede una parte contratante quedar obligada por un mensaje que ha sido enviado por una persona no autorizada?

Antes de seguir se deben identificar los supuestos de hecho a los que, bajo nuestro punto de vista, cabría aplicar este precepto:

- 1º Una conducta de fraude informático llevada a cabo desde un terminal de telecomunicación no perteneciente al autor del fraude y no afectando este fraude al titular del terminal.

- 2º Una conducta de fraude informático llevada a cabo desde el terminal de telecomunicación no perteneciente al autor del fraude y que produce perjuicio, dicho fraude, al titular del terminal.

- 3º Y, último supuesto, el uso subrepticio de un terminal de telecomunicación no como medio para la comisión de una defraudación patrimonial sino con ánimo exclusivamente defraudatorio en el uso de dicho terminal.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En el primer supuesto el titular del terminal se verá dañado únicamente por el coste económico derivado del uso indebido de la línea de telecomunicación. Por tanto la pena se referirá al daño que se inflige al titular del terminal de telecomunicación por el uso indebido del mismo. Los daños producidos por el fraude informático en sí deberán ser resarcidos con arreglo a otra normativa independiente. Ahora bien, cabría preguntarse si en la incriminación de la conducta de fraude informático el titular del terminal de telecomunicación no tiene una *culpa in vigilando* al no haber puesto los medios necesarios para evitar un uso fraudulento de su terminal. ¿Es correcto, desde un punto de vista político-criminal, hacer recaer toda la responsabilidad penal únicamente sobre aquél que de forma desautorizada ha utilizado el terminal?

En el segundo supuesto, creemos que, la situación cambia. El titular del terminal de telecomunicación no sólo sufre el daño patrimonial del uso no autorizado de este terminal sino también el perjuicio derivado de la actuación fraudulenta. Sería en estos casos en los que cabría apreciar un hipotético concurso de normas[68] entre aquella que tipificara el fraude patrimonial cometido por el medio informático y este artículo 254 que incrimina la defraudación en materia de telecomunicaciones. Entendemos que en la graduación de la pena, en este segundo supuesto, debe tenerse en cuenta el total del perjuicio ocasionado a la víctima pues el artículo 254 dice "ocasionando ... un perjuicio superior a cincuenta mil pesetas" sin especificar el origen de este perjuicio. Aquí también cabría hacerse otra pregunta: ¿ debería tenerse en consideración la ya aludida *culpa in vigilando* de la víctima para moderar la pena a imponer al reo?

El tercer y último supuesto contempla una conducta que podría calificarse de hurto de uso de un terminal de telecomunicación. Conducta ésta independiente al objeto de nuestro estudio.

Otros preceptos del Anteproyecto del 94 en los que se hace referencia a los

[68] La resolución de este concurso de normas y por tanto la determinación de la norma aplicable habría de observar el siguiente orden: el precepto especial se aplica con preferencia al general; el precepto subsidiario se aplica sólo en defecto del principal; el precepto penal más amplio o complejo absorbe a los que castiguen las infracciones consumidas en él; en defecto de los criterios anteriores el precepto penal más grave excluye a los que castiguen el hecho con pena menor.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

medios informáticos bien como objeto de ataque o como medio para la comisión de la conducta delictiva son los siguientes: artículo 261 dentro del capítulo dedicado al delito de daños el punto 2 establece que "*la misma pena se impondrá al que destruyere, alterare, inutilizare o de cualquier otro modo dañare los datos, programas o documentos electrónicos ajenos contenidos en soportes o sistemas informáticos, por cualquier medio*".

Una referencia indirecta a los documentos informáticos se recoge en el artículo 188 relativo al descubrimiento y revelación de secretos. La protección de las topografías de los productos semiconductores queda recogida en el punto 3 del artículo 268. Así mismo serán de aplicación al documento electrónico las disposiciones del capítulo relativo a las falsedades documentales, artículos 367 a 376. Por último se castiga en el artículo 377 la fabricación o tenencia de "programas de ordenador o aparatos específicamente destinados a la comisión de los delitos...". Por tanto el desarrollo de virus informáticos queda penado expresamente en este artículo. Se da, de este modo, respuesta penal a unas actuaciones que han supuesto graves pérdidas económicas y que pueden convertirse en una forma de fraude informático si se exige una contraprestación económica a cambio de no resultar infectado el sistema informático de la víctima.

Hasta aquí los antecedentes de Nuevo Código Penal que ha entrado en vigor el 25 de mayo de 1996.

LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, DEL CÓDIGO PENAL

Nuestro nuevo Código Penal, cuya trascendencia a nadie se le oculta, pues al definir los delitos y faltas define los presupuestos de la aplicación de la forma suprema que puede revestir el poder coactivo del Estado, es decir, la pena criminal.

Como la propia Exposición de Motivos del nuevo Código recoge, se ha afrontado la antinomia entre el principio de intervención mínima del Derecho Penal y las crecientes necesidades de tutela en una sociedad cada vez más compleja. Así tienen cabida en el nuevo texto formas de criminalidad hasta ahora huérfanas de regulación, como por ejemplo la introducción de nuevos delitos contra el orden socioeconómico, en concreto la estafa cometida a través de una manipulación

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

informática o artificio semejante. Esta apuesta clara del Código Penal por introducir en su texto nuevas formas delictivas relacionadas con la informática, se ha convertido en modelo para terceros países que todavía no han acogido estas figuras delictivas. Desde el punto de vista interno el nuevo C.P. es instrumento, se verá en un futuro si eficaz pero al menos sí con carácter preeminente en el ordenamiento jurídico español, para reprimir y controlar los riesgos que indudablemente se derivan del uso abusivo de las Tecnologías de la Información y las Comunicaciones.

Esquemáticamente, a continuación, se recogen las figuras delictivas del nuevo C.P. cometidas con la intervención del medio informático o en las que bienes o derechos relacionados con el tratamiento automático de la información son objeto de agresión. En ambos casos con derivaciones perjudiciales en el ámbito patrimonial de las víctimas.

Libro II, Título XIII, "**Delitos contra el patrimonio y el orden socioeconómico**", Capítulo II, "**De los robos**", a los efectos del delito de robo del artículo 238 que define el delito de robo con fuerza en las cosas como aquél ejecutado con uso de llave falsa, el artículo 239 considera llave falsa las **tarjetas magnéticas o perforadas**.

La Sentencia del Tribunal Supremo de 21 de abril de 1993, ya había calificado a la tarjeta de crédito como una verdadera llave puesto que permite el acceso al cajero poniendo en funcionamiento una operación de pago. La **utilización ilegítima de tarjeta de crédito o de débito o monedero electrónico, robada o extraviada,** por tercero, sería calificada como **robo con fuerza en las cosas**. De acuerdo con el artículo 240 el culpable de robo con fuerza en las cosas será castigado con la **pena de PRISIÓN de UNO a TRES AÑOS**. La pena puede **agravarse** pasando a **prisión de DOS a CINCO AÑOS** si, por ejemplo, se **pone** a la **víctima o a su familia en grave situación económica** o se haya realizado **abusando de las circunstancias personales de la víctima**. Lo que podríamos preguntar es ¿quién es la víctima?: el titular de la tarjeta o la entidad emisora. Ciertamente los fondos se detraerán de la cuenta de cargo asociada en tarjetas de débito o en tarjetas monedero, o bien se efectuará el correspondiente apunte en la cuenta de crédito en tarjetas de esta modalidad. Pero el titular, que observando la diligencia exigida en la custodia del instrumento de pago sufre un robo, hurto o extravío del mismo, no interviene en nada en la acción posterior y son las instalaciones (ATM, cajeros) de la entidad las que sufren el ataque haciendo que dicha entidad falte a uno de sus deberes básicos con su cliente, el deber de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

custodia del numerario.

Para estos supuestos el artículo 1.101 del Código Civil es claro al establecer que: *"quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren el tenor de aquéllas"*. La entidad tiene obligación de custodiar un numerario del que es propietaria cuando el cliente lo deposita en una cuenta corriente, libreta u otro producto de pasivo, y con más claridad en una cuenta de crédito. Por tanto la víctima es la entidad emisora debiendo quedar, a nuestro juicio, totalmente ajeno a la acción delictiva el titular de la tarjeta. En definitiva el que debe accionar en juicio será el establecimiento emisor no el sujeto titular del instrumento de pago, tarjeta, contra el autor/es de la infracción criminal.

Por otra parte, bajo nuestro punto de vista no siendo unánime la doctrina al respecto, el uso de tarjeta falsificada o la legítima manipulada debe calificarse como estafa informática y castigarse, por tanto, a través del artículo 248.2. del nuevo C.P. Para este tipo la pena es de PRISIÓN de 6 MESES a 4 AÑOS, si la cuantía de lo defraudado excediere de cincuenta mil pesetas. La mayor pena a imponer respecto del robo con fuerza en las cosas quedaría justificada por el mayor desvalor de las conductas que aquí consideramos, en las que el autor/es manipulan un instrumento de pago (tarjetas electrónicas) reconocido y protegido en el tráfico jurídico. Sostenemos esta interpretación al considerar la alteración de la tarjeta, o la creación de un nuevo instrumento falso, como una manipulación del *input* (de la entrada de los datos) incluido dentro del tipo del art. 248.2.

Por tanto el **uso fraudulento, irregular, de tarjetas electrónicas** existe, y bien puede quedar **tipificado como robo con fuerza en las cosas** (uso de tarjeta legítima por un tercero) o como **estafa** (uso de tarjeta falsificada o manipulada). El problema fundamental gravita en torno al descubrimiento del delincuente. Algunas entidades emisoras de instrumentos de pago, conscientes de esta dificultad, descargan la responsabilidad sobre el titular de la tarjeta si la disposición se llevó a cabo con **uso de NIP** (Número de Identificación Personal). Este es el punto de inflexión utilizado en la mayoría de los contratos de uso de tarjetas, de débito y algunas de crédito, para atribuir responsabilidad en la operación fraudulenta al titular del instrumento. Pero realmente el criterio de atribución de responsabilidad (uso del NIP) no reúne las garantías jurídicas

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

exigibles para apoyar una inversión de la carga de la prueba. Si el artículo 1.214, del Código civil, impone la carga de la prueba de las obligaciones al que reclama su cumplimiento, qué base jurídica asiste a aquellas cláusulas contractuales en la que si una operación con tarjeta se ha efectuado con uso de NIP el que tiene que probar que esa operación no se efectuó es el titular de la tarjeta, cuando resulta que el sistema implementado de uso de NIP no identifica a ese titular. No creemos que se pueda acudir a la autonomía de la voluntad de las partes (1.255 del Cc) cuando de contratos de adhesión se trata. Creemos merecen alguna reflexión añadida estas afirmaciones, que pasamos a efectuar.

Dada la trascendencia social del uso fraudulento, irregular, de tarjetas han sido y son, motivo de estudio y discusión fuera y dentro de España métodos de prevención de la obtención de tarjeta y número de identificación mediante sustracción y posterior utilización consiguiendo la disposición de numerario. Son hechos que quedan recogidos ya desde 1987 en la Memoria de la Fiscalía General del Estado y que pese a la controversia en torno a su exacta tipificación jurídico-penal no se encuentra obstáculo en su calificación como conductas delictivas (penalmente relevantes). El mismo Tribunal Supremo en Sentencia de su Sala 2ª, de 8 de mayo de 1992, enjuicia hechos relativos a una manipulación de cajero sito en la fachada de una entidad bancaria calificando dichos hechos como constitutivos de un delito de robo. A nadie se le oculta que el banco o caja que instala un cajero que permite la disposición de efectivo a quien porte una tarjeta y teclee un NIP (con el que no se identifica al disponente) asume voluntariamente el riesgo de entrega de dicho efectivo a persona no autorizada. Sin embargo este riesgo se asume y se reparten, a través de las cláusulas de los contratos de uso de tarjeta, las consecuencias del mismo. Del análisis de contratos de uso de tarjetas se puede concluir que, con casi absoluta generalidad, se incluyen unas cláusulas que no ya reparten sino que trasladan toda la responsabilidad al titular, si el uso de su tarjeta se realizó con NIP. Cláusulas de este tenor contravienen el espíritu y la letra del Código de Buena Conducta del Sector Bancario Europeo relativo a los Sistemas de Pago mediante tarjeta que el 14 de noviembre de 1990 firmaron las Asociaciones Europeas del Sector del Crédito (entre ellas AEB y CECA) donde expresamente se recoge que las cláusulas y condiciones contractuales que unen a emisor y titular de tarjetas "velarán por el **mantenimiento del equilibrio adecuado entre los intereses de las partes contratantes**". Cabría preguntarse si el NIP excluye toda posibilidad de uso fraudulento de la tarjeta. A nuestro juicio no, y bien caben algunas reflexiones al respecto.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

El número de identificación personal (NIP) NO es un medio que técnicamente garantice su uso exclusivo por su titular. Estos hechos son sistemáticamente desconocidos por entidades emisoras y responsables de redes de cajeros descargando en el usuario-titular la responsabilidad de toda disposición hecha con NIP. Con ello se vulnera el Código de Buena Conducta del Sector Bancario Europeo relativo a los Sistemas de Pago mediante Tarjeta ya que no permite establecer de forma automática la responsabilidad del titular por toda operación llevada a cabo con uso de NIP. Las disposiciones y pagos hechos con tarjeta, incluso con utilización del NIP, no garantizan que la disposición se efectúa únicamente por el titular de la tarjeta. **El NIP es un medio de legitimación y no de identificación**, sí se convertiría en medio de identificación incorporando por ejemplo la huella digital del titular.

La identificación de un sujeto debe basarse en tres pilares que en modo alguno actúan entre sí de modo excluyente. Por una parte lo que tiene el sujeto (la tarjeta que puede ser substraída), **lo que sabe** (el NIP que ha podido ser obtenido fraudulentamente) **y por lo que es** (una característica física, huella). En este último punto, al menos de momento, el vacío es total, el sistema se ha articulado sin prestar atención alguna a la incorporación de un medio de identificación personal del titular.

Pero avanzando un poco más, el hecho de mantener un sistema que permite la disposición de efectivo sin identificar al disponente vulnera la obligación de todo depositario (artículo 1.766 del Código Civil en relación con los artículos 1.094 y 1.101 del mismo cuerpo legal) de guardar la cosa dada en depósito. Indudablemente un depositario que no identifica al disponente no cumple con el tenor de su obligación y queda, conforme al citado artículo 1.101, sujeto a la indemnización de los daños y perjuicios causados. Bien, hemos llegado a un punto por otra parte obvio, si la **firma de un documento por su autor ha sido tradicionalmente la forma de constatar la autoría y la integridad del mismo la constatación de la autoría e integridad de una operación desde cajero necesita abarcar los dos ámbitos: identificación e integridad.** La identificación sufre la grave laguna expuesta pero la integridad del mensaje tampoco queda garantizada.

Debe tenerse en cuenta que en una operación desde cajero hay una transmisión de datos por un canal de comunicación como es, por ejemplo, la línea telefónica

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

convencional que no es en principio seguro "per se".

Centrándonos en las transacciones desde cajero automático nos encontramos con uno de los secretos mejor guardados: la seguridad en la transmisión de los datos en una operación realizada desde cajero. Indudablemente es importante la seguridad del recinto en el que se encuentra instalado el cajero. La conveniencia de que se trate de un recinto físicamente seguro a lo que sin duda contribuye la instalación de una cámara de vídeo que pueda identificar en cada momento al disponente. Pero ahora no adoptaremos esta perspectiva sino aquella otra de la que tan poco se habla: lo que pasa "detrás" del cajero. Con ánimo simplificador en una operación desde cajero automático se produce una transmisión de datos desde el terminal (cajero) hasta el centro resolutor que valida la operación. La información puede encontrarse en tres estados: almacenada, en proceso o bien transmitiéndose. Bien, es en este último estado donde es más vulnerable. Es aquí donde se plantea la seguridad del sistema de información. No procederemos a una evaluación de los niveles de seguridad de los sistemas de transmisión de información en las redes de cajeros, dada la parquedad de datos con la que contamos no por falta de investigación, pero sí expondremos las bases sobre las que procede hacer dicha evaluación .

En un sistema de información deben garantizarse de una forma razonable los tres grandes vectores de la seguridad de la información: la integridad de los datos, la confidencialidad (donde debe incluirse autentificación y no-repudio) y disponibilidad. Se han adoptado sistemas criptográficos simétricos en buena parte de las redes de cajeros, sistemas que protegen los datos frente a ataques pasivos pero no frente ataques activos, es decir, se garantiza la confidencialidad pero no la integridad de la información transmitida. Sin exigir más de lo que la ley exige, custodia diligente y entrega de los fondos a su titular, únicamente la **firma digital (electrónica)**[69] basada en **sistemas de criptografía asimétrica** garantizaría

[69] Con independencia de tratar esta medida de seguridad lógica en el punto 4 de este trabajo, caben ahora hacer algunas precisiones sobre el concepto de firma digital. La firma digital o electrónica es una cadena de bits que reúne las tres características fundamentales de una firma manuscrita, a saber: identifica al firmante, cumple una función de acuerdo o aquiescencia con el contenido de lo firmado y, por último, cumple una función probatoria pudiendo comprobarse posteriormente su autoría. Las relaciones civiles y mercantiles que se desarrollan en un contexto electrónico necesitan de este medio de autentificación. La implantación de esta firma digital se basa en sistemas de encriptación asimétrica de clave pública. La criptografía es una rama del conocimiento muy antigua, con

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

adecuadamente la integridad de los datos en una operación desde cajero automático. Lo que en términos de justo equilibrio de las contraprestaciones no parece admisible es poner en funcionamiento un sistema de disposición de efectivo que no identifica adecuadamente al disponente, que no garantiza la integridad de los datos que se transmiten entre el cajero y el centro de validación y hacer descansar toda la responsabilidad sobre el titular si media el uso del número de identificación personal que, a nuestro juicio, ni identifica ni garantiza la integridad de la operación. En los contratos de uso de las tarjetas se suele invertir la carga de la prueba (como ya hemos visto de acuerdo con el artículo 1.214 del Código Civil la prueba de las obligaciones incumbe al que reclama su cumplimiento) y lo que es responsabilidad del emisor, garantizar la integridad y autenticidad de la operación, justificar la existencia de la obligación, se presume si se ha utilizado el NIP.

En conclusión el sistema de disposición de efectivo en cajeros automáticos y de pago con tarjetas en comercio no permite en una posible controversia entre las partes probar, en todo caso, la existencia de la operación y su contenido. Por

---

amplio desarrollo en el ámbito militar y que proporciona seguridad en la transmisión de mensajes. En la criptografía moderna existen dos tipos de criptosistemas: el simétrico o de clave privada y el asimétrico o de clave pública. En el simétrico hay una sola clave que sirve tanto para cifrar el mensaje a transmitir como para descifrarlo por el receptor. En el sistema asimétrico cada extremo de la transmisión (emisor y receptor del mensaje) tiene dos claves una pública para el cifrado y otra privada para el descifrado. Las claves públicas como su propio nombre indica son accesibles para todos los usuarios, cada uno tiene la suya conocida por el resto, y las claves privadas son secretas, cada usuario tiene la suya que no es conocida por el resto. Al funcionar estas claves siempre por pares proporcionan dos servicios fundamentales: servir de "sobre seguro" para el mensaje que envían a un usuario y de FIRMA de lo que ese usuario envía. Un mensaje encriptado con la clave pública de un usuario sólo podrá ser descifrado con la clave privada de ese usuario que sólo él conoce. Por tanto encriptar con la clave pública de un usuario proporciona un servicio de "sobre seguro" para el mensaje encriptado con destino a dicho usuario. Por otra parte al encriptar un mensaje un usuario con su clave secreta-privada el resto que descifren con la clave pública del primero tendrán la certeza de que el titular de la clave privada emitió el mensaje, FIRMÓ el mensaje. En cualquier caso los sistemas asimétricos se construyen de forma que cualquier usuario puede cifrar un mensaje con su clave privada de descifrado y recuperar dicho mensaje otro usuario con la clave pública del primer usuario. De este modo la autentificación, no repudio, integridad y confidencialidad del mensaje quedan garantizadas. Cfr. INZA ALDAZ, Julián. *"Firma Electrónica"*. Mundo Internet 97. II Congreso Nacional de Usuarios de Internet e Infovía. Libro de Ponencias. Madrid. Febrero 1997. Página 113 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

tanto una posible estrategia de defensa es la creación de la duda que se puede disipar completamente con la implantación de las soluciones que la técnica ofrece. No en todas las redes se ha implementado un sistema que permita probar que un determinado titular de tarjeta emitió la operación, que esa operación tiene un determinado contenido y que el centro resolutor recibió la operación en los términos emitidos por el titular u ordenante de la operación. Sin embargo técnicamente (con los sistemas de criptografía asimétrica apuntados combinados con la identificación a través de característica personal) es posible que tanto el titular de la tarjeta, o el ordenante de la operación, como el centro de validación puedan probar la existencia y contenido de la operación ordenada sin que ninguno de los dos pueda eliminar la operación o alterar sus términos. Con ello se resolvería uno de los escollos fundamentales en la persecución del uso fraudulento de tarjetas electrónicas como es el descubrimiento del autor de los hechos y la consiguiente atribución de responsabilidades civiles y penales.

La exigencia por las propias entidades de destrucción material de la tarjeta una vez transcurrido su plazo de vigencia no hace sino evidenciar la "debilidad" en la seguridad de las tarjetas con banda magnética.

Por lo expuesto sostenemos que la solución a la manipulación y uso fraudulento de tarjetas debe venir de la mano de fortalecer la seguridad intrínseca y extrínseca de la propia tarjeta, y ello pasa por introducir, entre otras, auténticas medidas de identificación del titular de la tarjeta. Con esto tocamos uno de los puntos relacionados con una cuestión de la más candente actualidad: las tarjetas inteligentes, tarjetas "chip", y una de sus aplicaciones más conocida el monedero electrónico.

Breves reflexiones sobre el MONEDERO ELECTRÓNICO:

Nos hemos acostumbrado, aunque sea de manera inconsciente, a vivir en un ambiente tecnológico donde la injerencia de la informática en nuestra vida se ha hecho cada vez más extendida y difusa. El registro de las adquisiciones comerciales realizadas con tarjetas de crédito, el procesamiento informático de nuestros datos bancarios son, entre otros muchos, algunos ejemplos de la omnipresencia de la informática en nuestra vida cotidiana. Cabría hablar de "un juicio universal permanente", como apunta Frosini, al que nos encontramos

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

sometidos aunque no reparemos en ello. Con estas líneas queremos llamar la atención sobre la potencial agresividad sobre la vida privada de su titular de las tarjetas con microprocesador, base del nuevo producto del monedero electrónico. Como característica fundamental diferenciadora respecto de las tarjetas con banda magnética la tarjeta con microprocesador incorpora una importante capacidad de almacenamiento o memoria que exige el diseño de un sistema de seguridad que garantice la integridad, confidencialidad tanto de los datos como de las comunicaciones que con base en dichos datos se efectúen.

Con la extensión de las tarjetas inteligentes la funcionalidad (ámbitos de aplicación) de estos instrumentos se multiplica en comparación con las tradicionales tarjetas de débito y crédito. Es indudable que podrán absorber las funciones de éstas, pero junto a ellas se enmarcan otras como archivo de datos personales, sistema de acceso a ficheros centralizados (de carácter financiero o extrafinanciero), dinero electrónico etc... Pueden llegar a convertirse estas tarjetas inteligentes en una reproducción electrónica de cada individuo, por ejemplo, la incorporación a una tarjeta con chip del historial médico de su titular exige unos niveles de seguridad muy superiores a los actualmente existentes. Baste para ello remitirse a las exigencias de seguridad que en relación con el tratamiento automatizado de los datos personales establece el artículo 9 de la L.O. 5/1992, de 29 de octubre.

Así pues la denominada tarjeta chip o tarjeta inteligente presenta unas claras diferencias respecto de la tarjeta magnética tradicional. Con ánimo siempre simplificador podrían clasificarse estas diferencias en tres grupos:

1. Diferencias físicas: la tarjeta inteligente lleva incorporado un chip. Un chip (microprocesador) o elemento de actividad de la tarjeta. Junto a los componentes del chip que se ocupan del control y gestión de los datos se encuentra la memoria. Aquí radica una de las mayores diferencias respecto de la tarjeta con banda magnética en las que la capacidad de almacenamiento es mínima.

2. Diferencias en cuanto a la seguridad: el incremento de la seguridad en las tarjetas inteligentes se extiende a dos ámbitos, la seguridad física y la seguridad lógica. El incremento en la seguridad física se basa en la incorporación en la tarjeta de unas memorias ROM y EPROM no volátiles en

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

las que se almacenan datos e instrucciones concretas para el funcionamiento de la tarjeta y datos propios del usuario. La capacidad de almacenamiento que incorporan las tarjetas chip sin duda proporciona la base para resolver uno de los vacíos más evidentes que en relación a la identificación del titular presentan las actuales tarjetas de banda magnética. No se intenta presentar como la panacea de todos los supuestos de uso abusivo de tarjetas la incorporación en las mismas de características de identificación biométricas pero es indudable que pueden evitarse determinadas prácticas fraudulentas. Sin ser el único entre los sistemas de identificación el dactilar cuenta actualmente con un avanzado desarrollo técnico. El objetivo de todo sistema de identificación dactilar es establecer un procedimiento automático para determinar, a partir de dos huellas, si éstas son equivalentes, es decir, si corresponden a una misma persona aunque tomadas en distintos momentos. Estos sistemas están sujetos a un margen de error o tasas de error. Estas tasas de error pueden corresponder a dos situaciones falsa aceptación y falso rechazo. Se puede afirmar, con base en una evaluación de los sistemas en funcionamiento, que la frecuencia de situaciones en las que se produce un falso rechazo, es decir dos huellas realmente equivalentes no se reconocen como tal, es muy superior a errores del sistema por falsa aceptación. Por tanto el intrusismo se evita por el sistema en un alto porcentaje de ocasiones. En definitiva el sistema no es infalible pero debemos tener en cuenta que en seguridad no se puede hablar en términos absolutos pero sí una vez identificada la debilidad mitigarla con los medios técnicos existentes.

Por otra parte el incremento de la seguridad lógica, en tarjetas con chip, se manifiesta en la encriptación de todas las comunicaciones que se efectúen con la tarjeta. Sin embargo conviene recordar que las exigencias de seguridad en estas comunicaciones exige atender a cuatro puntos fundamentales: autenticación (garantizar que los comunicantes son realmente quienes dicen ser), integridad (no alterabilidad de los datos en la comunicación), confidencialidad (no accesibilidad del contenido de la comunicación por terceros) y no repudio (imposibilidad de que un comunicante niegue su intervención). Afirmar que todas las comunicaciones que se efectúen con tarjeta inteligente se encuentran encriptadas en sí no es decir nada ya que hay que atender al criptosistema utilizado. Sólo un criptosistema de clave pública o asimétrico (ya comentado más arriba) permite garantizar los cuatro puntos precitados.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3. Diferencias de funcionalidad.

De momento las funciones asignadas a las tarjetas chip serán muy limitadas, se utilizarán como tarjetas "prepagadas" o tarjetas monedero (una modalidad de tarjetas de débito, en definitiva), pero sus funciones como se ha dejado entrever pueden ser mucho más amplias.

El abanico de operaciones y funciones asignadas al "plástico" se amplía y consideramos inaplazable su regulación específica en derecho español, aunque bien es cierto que el Nuevo Código Penal recoge en los tipos de robo con fuerza en las cosas y falsificación de moneda[70] referencia expresa a las tarjetas de crédito y débito. Desde 1978 en Estados Unidos la *Electronic Fund Transfer Act* regula dentro del ámbito más amplio de la transferencia electrónica de fondos las consecuencias jurídicas de las relaciones entre entidades y titulares de tarjetas. Así mismo el Instituto Monetario Europeo (IME) publicó un informe advirtiendo de las consecuencias de las nuevas tarjetas monedero sobre el nivel de circulación de moneda de curso legal y su consecuente repercusión sobre el monopolio de emisión que en dicho ámbito ostentan los bancos centrales, en nuestro país el Banco de España.

Las cuestiones apuntadas en relación con las tarjetas monedero y tarjetas inteligentes en general son múltiples, su análisis complejo y el vacío legal alarmante, salvo la encomiable inclusión en el Nuevo Código Penal de algunos preceptos (239, 248, 387) que castigan delitos relacionados con estos instrumentos de pago.

- **Libro II, Título XIII**, "Delitos contra el patrimonio y contra el orden socioeconómico", Capítulo VI, "De las defraudaciones", Sección 1ª, "De las estafas", **art. 248.2** tipifica la denominada "**ESTAFA INFORMÁTICA**". La redacción del tipo es amplia lo que permite englobar la compleja casuística de

[70] Nuevo Código Penal, artículo 387, dentro del Capítulo relativo a la falsificación de moneda y efectos timbrados. "*A los efectos del artículo anterior se entiende por moneda la metálica y papel moneda de curso legal. A los mismos efectos se considerarán moneda las tarjetas de crédito, las de débito y los cheques de viaje. Igualmente, se equipararán a la moneda nacional, la de la Unión Europea y las extranjeras* ".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

fraudes cometidos a través de las Tecnologías de la Información y las Comunicaciones. El art. 248.2 introduce como novedad respecto de los textos prelegislativos la expresión "artificio semejante" ampliando el medio comisivo.

Como elemento subjetivo del tipo se exige el ANIMO de LUCRO. La estafa informática se configura como un delito de tendencia, exigiéndose para la calificación de antijurídicas de estas conductas el ánimo de lucro del autor/es. Este ánimo de lucro determina, así mismo, la diferencia respecto del delito de daños. La utilización del tipo de la estafa excluye la posibilidad de comisión culposa. La Jurisprudencia antes del nuevo C.P., calificaba estas acciones como delitos de apropiación indebida dado que la aplicación del tipo de la estafa encontraba la importante dificultad de exigir el "engaño" y no ser susceptibles de engaño las máquinas.

Atendiendo a otro supuesto de hecho, como más adelante veremos, la Jurisprudencia del Tribunal Supremo en Sentencia de 25 de junio de 1985 castigó como estafa el abuso de tarjetas de crédito obteniendo mercancía a sabiendas de que no se pagará.

- **Título XII, Capítulo IX**, "De los daños", **art. 264** establece que *"se impondrá la pena de prisión de uno a tres años y multa de doce a veinticuatro meses al que por cualquier medio **destruya, altere, inutilice** o de cualquier otro modo **dañe los datos, programas o documentos electrónicos ajenos** contenidos en redes, soportes o sistemas informáticos"*. Sin lugar a dudas queda tipificado el **SABOTAJE INFORMÁTICO** sin regulación hasta el momento.

- **Título XVIII**, "De las Falsedades", **Capítulo I**, "De la Falsificación de Moneda y Efectos Timbrados", el **artículo 386** castiga con penas de Prisión de OCHO a DOCE AÑOS la fabricación de moneda falsa. El **artículo 387** recoge expresamente que *"... se entiende por moneda la metálica y papel moneda de curso legal. A los mismos efectos se considerarán moneda las tarjetas de crédito, las de débito"*.

Cabe sin dificultad considerar incluidas las tarjetas monedero (que son una modalidad de tarjeta de débito), mayores dificultades presenta el denominado dinero electrónico o dinero virtual utilizado dentro de la red Internet. Para poder

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

utilizar este dinero virtual ha de solicitarse al banco que todo o parte del dinero existente en una cuenta, u otro producto de pasivo, se transfiera a Internet donde tendremos nuestra propia cartera o banco personal. La manipulación y/o alteración de este dinero virtual no queda tipificada con claridad en el artículo 387 (falsificación de moneda) aunque entendemos cabría el castigo de estas conductas a través del párrafo segundo del artículo 248 (delito de estafa).

- **El Capítulo II, del mismo Título XVIII**, castiga a partir del **artículo 390** las falsedades documentales.

La falsificación de documentos electrónicos quedaría amparada por estos artículos desde el momento que el artículo 26 del mismo Código establece que: *"A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"*.

Indudablemente un soporte material con eficacia probatoria y relevancia jurídica es el soporte informático. Así claramente lo establece, en el ámbito del Derecho público, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en su artículo 45.5. Según este artículo gozan de validez y eficacia de documento original los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos. Esta validez y eficacia de documento original será posible siempre que quede garantizada su autenticidad, integridad, conservación y la recepción por el interesado. Estos mismos requisitos son exigidos por el artículo 6 del Real Decreto 263/1996 que desarrolla esta artículo 45.
Por lo expuesto queda claro que un documento electrónico, informático o telemático goza de relevancia jurídica en el ámbito del derecho administrativo y por tanto cuenta con protección en el ámbito penal.

Una vez comentados, sucintamente, los antecedentes y la vigente regulación de los delitos relacionados con sistemas y medios informáticos creemos conveniente recoger algunas declaraciones de la Jurisprudencia del Tribunal Supremo en torno a las conductas denominadas de fraude informático. Así mismo, se incluye un análisis de la jurisprudencia menor (Audiencias Provinciales) más reciente en relación con uso abusivo de tarjetas electrónicas. Las pretensiones derivadas de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

estos últimos hechos en su mayoría vienen ventilándose en el orden civil, por tanto entre emisores y titulares de tarjetas, ante el desconocimiento de los autores materiales de la acción delictiva .

2.2. CONCEPTO EN LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO ESPAÑOL. (Referencia a jurisprudencia menor en relación con el uso abusivo de medios de pago)

* Jurisprudencia del Tribunal Supremo

Pocas son estas declaraciones, puesto que pocas de estas conductas llegan a hacerse públicas. La llamada "cifra negra[71]" en la criminalidad informática y en concreto en las conductas fraudulentas relacionadas con el empleo de medios informáticos, es uno de los obstáculos con los que se encuentra el estudioso o simplemente el interesado por estos temas. Como DeMaio[72] pone de manifiesto, esta realidad hay que abordarla desde la respuesta a una pregunta sencilla: ¿es conveniente dar noticia a las autoridades policiales de un ataque a nuestro sistema informático? Parece evidente que si alguien está violando la ley y tenemos conocimiento de ello debemos denunciar los hechos. Pero a veces lo que es más

[71] El número de fraudes informáticos denunciados es bajísimo. Algunos expertos estiman que únicamente se descubren el 15 % de los fraudes, y no más de un 20% de los descubiertos son denunciados. En este tema de la cifra negra de los fraudes informáticos nos encontramos con un doble problema: primero para las empresas supone una grave pérdida de imagen que se llegue a conocer la vulneración de su sistema de seguridad informático. Y segundo el intercambio de información sobre los delitos informáticos puede contribuir a la ampliación y difusión de la vulnerabilidad informática. La difusión masiva de las particularidades acaecidas en un determinado fraude informático puede favorecer la repetición de esa misma conducta delictiva por otras personas. Nos indica Pérez Gómez que en Estados Unidos el FBI y las autoridades judiciales han entendido que debe restringirse el acceso a toda información relacionada con la comisión de un fraude informático. De este modo vemos como las causas de la falta de datos fiables sobre estos delitos responden a diversos factores tanto de autoprotección de las mismas víctimas como externos de políticas de lucha contra este tipo de delincuencia. Cfr. Pérez Gómez, J.M. *La Organización Empresarial ante los Fraudes Informáticos.* ESIC-MARKET. 1988, 61 julio - septiembre. Pág. 91 y ss.

[72] DEMAIO, Harry B. *Information Protection and other Unnatural Acts. Every manager's guide to keeping vital computer data safe and sound.* AMACOM. American Management Association. New York. 1992. Pág. 181 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

evidente no es lo mejor ya que existen algunas cuestiones adyacentes que deben tenerse en cuenta. Por ejemplo: ¿realmente puede la policía hacer algo eficaz en la represión de estas conductas?, o si se quiere plantear la pregunta con mayor claridad, ¿dispone la policía de métodos apropiados para investigar y llegar al fondo de los hechos en los que se ha visto agredida la integridad de un sistema informático?

DeMaio haciendo referencia a la realidad estadounidense reconoce que aun muchas comisarías no pueden llevar con eficacia la investigación y esclarecimiento de los hechos en estos ataques a sistemas informáticos. No existe personal cualificado para su persecución, a veces no se confiere la suficiente importancia a estas conductas. A esto hay que añadir un problema más, si el denunciante no está dispuesto a continuar hasta el final del proceso es preferible no denunciar al supuesto autor de los hechos. Porque si no se llega hasta el final lo único que se conseguirá es una publicidad del caso sin solución satisfactoria para el afectado.

Quizá sea más conveniente, controlar la vía de ataque y posteriormente denunciar. Si se denuncia sin controlar previamente, el atacado se encuentra en las manos de cualquier otro desaprensivo que quiera repetir la acción delictiva.

Con esta vía de razonamiento el autor llega a dar una interpretación , pensamos, bastante aproximada de la causa de la falta de publicidad de estos hechos. Pueden existir razones que hagan conveniente mantener en secreto un ataque a un sistema informático hasta tanto no sea este ataque controlado y bien conocido. Es comprensible que una empresa, entidad financiera, organismo público etc..., no quiera que se haga pública la vulnerabilidad de su sistema informático hasta tanto esta vulnerabilidad no haya sido controlada o subsanada.

Quizá no sea un mal método, para tomar conciencia del peligro que suponen este tipo de conductas delictivas relacionadas con la informática, tratar de trasladar 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

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

conocidos por la Jurisprudencia de nuestro Tribunal Supremo y que ayudan a apreciar con mayor cercanía el fenómeno del fraude informático.

Entrando ya en el estudio de estas declaraciones del Tribunal Supremo sobre fraudes informáticos merecen especial mención las siguientes Sentencias: 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.

La **Sentencia de 14 de enero de 1987** no criminaliza el supuesto de hecho que enjuicia. Se trata de una Sentencia de la sala de lo social del Tribunal Supremo. En ella se considera como causa justa para el despido la transgresión de la buena fe contractual y el abuso de confianza procedente de un fraude en la utilización de los ordenadores. Para el Tribunal Supremo queda evidenciada una realidad de deslealtad para con la empresa y de quebrantamiento de la buena fe al manipular el empleado las cuentas de haberes utilizando el terminal de teleproceso de su oficina. Reconoce la Sentencia que esta conducta incluso podría ser merecedora de sanción penal dada su trascendencia económica. No obstante es interesante estudiar esta declaración jurisprudencial por dos razones fundamentales: primero usa la expresión de fraude informático como delimitadora de un nuevo grupo de conductas delictivas y segundo reconoce como substrato necesario al fraude informático la existencia de una relación de confianza previa entre defraudador y defraudado. A continuación veremos cómo, a nuestro juicio, esta relación de confianza es un elemento básico diferenciador del fraude informático.

La **Sentencia de 8 de octubre de 1988** al igual que la anterior de la Sala de lo social del Tribunal Supremo no criminaliza los hechos pero sí entiende que son constitutivos de una falta muy grave de transgresión de la buena fe y abuso de confianza en el desempeño del trabajo. En este caso el empleado comete lo que la doctrina denomina un hurto de uso de tiempo del ordenador. Es decir, el empleado utiliza el ordenador de la empresa donde trabaja para fines propios produciendo un daño a su empresa. Si este daño no se hubiera producido el trabajador no habría cometido falta grave pues el hurto de uso no es penalizable en nuestro derecho salvo en el caso de los vehículos de motor. Esta conducta constituye una forma más leve de fraude ya que aquí el interés económico se limita al uso para fines particulares del ordenador de la empresa.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En la **Sentencia de 8 de noviembre de 1989** el procesado A.G.L., empleado del Banco Urquijo Unión, S.A., venía desempeñando las labores propias de oficial administrativo, siendo uno de los empleados más antiguos de la sucursal en la que prestaba sus servicios. En el segundo semestre del año mil novecientos ochenta y cuatro, trabajando en el equipo informático utilizado en la entidad bancaria para la práctica de todo tipo de asientos contables, y dada su habilidad laboral pudo, en fechas no precisadas con exactitud, pero con anterioridad al veintiséis de octubre de mil novecientos ochenta y cuatro, **manipular** en varias cuentas particulares realizando cargos y abonos así como regularizaciones y cancelaciones no interesadas por sus legítimos titulares, ni autorizadas por el Banco, así como varias extracciones en forma de cheque al portador. Los beneficios obtenidos por todas estas manipulaciones eran transferidos a una cuenta corriente abierta a su nombre, o a una cartilla cuyo titular era su esposa, desconocedora de su proceder.

Estas alteraciones en las cuentas fueron detectadas a partir del cambio en la dirección de la oficina bancaria en julio de mil novecientos ochenta y cuatro. Al ser requeridos por el nuevo director una serie de datos, éstos dieron la posibilidad de detectar algunas anomalías. Como consecuencia de dicha detección se investigó la autoría de estas irregularidades y sospechando fuera su autor el ahora procesado, A.G.L., éste fue convocado a una reunión con el director de la oficina bancaria confesando, en dicha reunión, que había manipulado las cuentas realizando los hechos antes relatados.

La Audiencia de instancia condenó a A.G.L. como autor responsable de un delito de falsedad y un delito de hurto, con la concurrencia de la circunstancia modificativa agravante de abuso de confianza. Se le impusieron penas privativas de libertad, pecuniarias y las accesorias de suspensión del derecho de sufragio **¡Error! Marcador no definido.**y del ejercicio de todo cargo público por el tiempo de la condena así como el pago de las costas procesales.

La aplicación de la agravante de abuso de confianza se fundamenta en el presente caso por el quebrantamiento de los deberes éticos y morales inherentes a toda relación laboral y aprovechamiento de las facilidades que proporciona la situación de dependencia. Estas circunstancias facilitaron la realización de las manipulaciones contables y el apoderamiento de las sumas de dinero precisadas en el "factum", en el relato de los hechos probados.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Se recogen por tanto en esta sentencia del Tribunal Supremo unos hechos constitutivos de una de las formas típicas del denominado fraude por ordenador, la manipulación de los datos de entrada, "in put", en el sistema informático que provocan el devengo de una serie de sumas de dinero a favor del autor de la manipulación.

El Tribunal que conoce en primera instancia de los hechos y el mismo Tribunal Supremo están de acuerdo en calificar jurídicamente los hechos como constitutivos de un delito de falsedad. No entran por tanto en la calificación de estos hechos como constitutivos de un delito de estafa o de fraude. A nuestro entender en la calificación se produce una apreciación parcial de los hechos ocurridos. Es cierto que el procesado falsea unos datos para tener acceso a una serie de cuentas corrientes, es decir, lleva a cabo una conducta fraudulenta, pero no se debe olvidar que en los hechos concurren otra serie de circunstancias que permitiría calificarlos como de auténtico fraude informático. Así pues repasaremos estas circunstancias: se lleva a cabo una conducta de manipulación con ánimo de lucro ilícito, se produce un perjuicio para otro, en este caso el Banco Urquijo Unión, S.A. y la intervención de los componentes físicos y lógicos del sistema informático son instrumento necesario para la comisión de los hechos delictivos.

Sabemos que el fraude no es una figura jurídico-positiva con un contenido preestablecido, sino que por el contrario nos movemos en un terreno poco explorado jurídicamente y todavía no enmarcado en una categoría de derecho positivo concreta. Hemos analizado cómo el Proyecto de 1992 recoge una figura cercana cual es la de la estafa informática, pero nada se habla en este texto legal de la figura del fraude informático, ni tampoco en el Anteproyecto del 94. ¿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 ambos delitos?

Parece que la noción de fraude lleva consigo la existencia de una relación de poder especial sobre el objeto defraudado, lo que en la sentencia se alude 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

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 que es 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. Indudablemente tras la promulgación del nuevo Código Penal el tipo de la estafa engloba estas conductas no haciendo la distinción entre fraude y estafa que aquí apuntamos.

Un supuesto de hecho semejante al de esta Sentencia de 8 de noviembre de 1989, aunque con un matiz diferenciador fundamental es el que recoge 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 agravante específica de especial gravedad por

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

la cuantía de la defraudación[73].

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[74] y por un delito continuado[75] de apropiación indebida. En esta segunda Sentencia también se aprecia la agravante específica de especial

[73] 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.

[74] 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 pueden "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 carácter 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."

[75] La esencia del delito continuado , como así pone de manifiesto la Sentencia del Tribunal Supremo de 28 de enero de 1993, radica en una pluralidad de acciones u omisiones que infrinjan el mismo o semejantes preceptos penales, ligadas por un plan preconcebido o dolo unitario, que sirve de "abrazadera a las diversas infracciones y que justifica el tratamiento de unicidad que se les prodiga". Por tanto para que venga en aplicación lo establecido en el artículo 69 bis del Código Penal y por tanto apreciar la existencia de delito continuado es necesario: 1°. La existencia de un solo sujeto activo de todas las acciones realizadas. 2°. Obrar con un dolo unitario. 3°. Homogeneidad del bien jurídico protegido. 4°. Semejanza en el precepto penal violado, y 5°. Conexión espacio-temporal. Todos estos requisitos concurren en el caso que se viene comentando matizada la conducta por la utilización de medios informáticos en la comisión del delito.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

gravedad, en razón a 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 no porque se tenga en cuenta la circunstancia personal del autor de los hechos que desempeña el cargo de apoderado del Banco, sino porque el engaño, elemento fundamental en la estafa, no puede afectar a máquinas[76]. La Sentencia continúa diciendo 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 una parte, dentro del concepto de documento a los soportes informáticos, y reconocer su protegibilidad jurídica. Y por otra parte se hace una primera calificación de los hechos como constitutivos de un delito de estafa. La manipulación dolosa de información en este supuesto se hace con la intención de dar una apariencia de legalidad a unas sumas de dinero que previamente han sido apropiadas. La manipulación dolosa de información no se hace con la intención de llevar a otro a un error e inducirle a realizar una disposición patrimonial. Por tanto la aplicación del delito de estafa del artículo 528 del Código Penal no es adecuada. El delito de estafa vendría en aplicación si se tratara de una manipulación de datos de entrada como consecuencia de la cual un sujeto lleva a cabo un acto de disposición. El Tribunal Supremo no hace esta apreciación pero, sin embargo, sí cambia la calificación de los hechos haciéndolos merecedores de

[76] En este sentido el Prof. ROMEO CASABONA señala como algunos elementos del tipo de la estafa, como el engaño y el error, "han de recaer y originarse sucesiva y exclusivamente en un individuo". Las manipulaciones informáticas, de acuerdo con estas consideraciones, no reunirán los requisitos para calificarse como estafa al no poder apreciar el engaño sobre una persona. "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. Páginas 58 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

la pena del delito de apropiación indebida. Se vuelve en este caso a la situación ya descrita en una Sentencia anterior al calificar como de apropiación indebida, y no como estafa, unos hechos en los que el autor de los mismos aprovecha una relación de poder especial para cometer el hecho delictivo. Si la manipulación la hubiera llevado a cabo sobre el programa que gestiona la administración de los fondos del banco, al no existir intervención de una persona no hay engaño a otro y por tanto no se podría aplicar el delito de estafa (hoy con la nueva tipificación del delito de estafa sí), en este caso vendría en aplicación el tipo de hurto o de apropiación indebida según las circunstancias del caso.

Otro supuesto de manipulación de los datos de entrada en un proceso informático que ocasiona la manipulación, o falseamiento, del resultado del proceso lo constituyen los hechos probados de la Sentencia de **16 de septiembre de 1991** del Tribunal Supremo. En esta Sentencia los hechos se centran en la alteración de la contabilidad de una empresa por uno de sus empleados. El empleado hacía constar deliberadamente en las hojas de caja una cantidad inferior a la verdadera suma del total de los albaranes recibidos en ese día, apropiándose de la diferencia. La manipulación del "in put" se produce al alterar el resumen de los ingresos en las hojas diarias. Se condenó al autor de estos hechos en primera instancia por un delito de apropiación indebida y por otro de falsedad en documento mercantil. Esta Sentencia se recurrió en casación ante el Tribunal Supremo desestimando éste todos los motivos de casación alegados por las partes salvo uno que solicitaba la apreciación de una circunstancia atenuante que finalmente se aprecia y confirmando la calificación de los hechos que efectuó la Audiencia. En esta Sentencia se enjuicia de nuevo un supuesto de manipulación del proceso informático que se castiga penalmente acudiendo a alguna de las figuras tradicionales, en este caso la apropiación indebida. La frecuencia e importancia que han adquirido ya este tipo de hechos delictivos cada vez reclama con más fuerza una regulación específica para estos supuestos. Y de hecho así se ha producido con la aprobación del nuevo Código Penal y la inclusión en el mismo del delito de estafa informática en su artículo 248.2.

Pasando ya al análisis de la **Sentencia de fecha 25 de enero de 1994**, merece resaltar en ella la tipificación de los hechos por el Tribunal como constitutivos de un delito de malversación de fondos más cercano al tipo penal del fraude que al de falsedad, con el que la Sentencia anterior tipificaba los hechos.
Los hechos se pueden resumir del siguiente modo: la procesada P.A.P. venía

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

trabajando desde agosto de mil novecientos ochenta y ocho en la Subdirección de Prestaciones del Instituto Nacional de Empleo de Pamplona, en calidad de auxiliar administrativo. En esta Subdirección se tramitaban las altas y bajas en las prestaciones de desempleo mediante la introducción de datos en el ordenador o sistema informático. La procesada manejaba el ordenador a los fines señalados en materia de prestaciones. Con el propósito de obtener un beneficio económico introdujo en el ordenador, como beneficiarias de prestaciones por desempleo, a una serie de mujeres que no tenían derecho a dichas prestaciones sin el conocimiento de éstas. Todas estas manipulaciones las llevó a cabo la procesada sin autorización de sus superiores y sin soporte administrativo alguno. La procesada daba de baja a algunas de estas supuestas beneficiarias cuando el alta ya la había transmitido al ordenador y había generado sus efectos propios, es decir, la orden de pago a una entidad bancaria. De este modo facilitaba la ocultación de los hechos delictivos y dificultaba su descubrimiento. Se debe tener en cuenta que de estas manipulaciones no quedaba rastro de su comisión en el sistema informático, favoreciéndose así su impunidad.

Asimismo P.A.P. utilizaba, como otros medios de ocultación de su conducta, el código de terminalista de otro empleado o funcionario del INEM o bien aprovechaba el tiempo en que la pantalla del ordenador se encontraba en fase de "time out". De este modo conseguía que el sistema librase las pertinentes órdenes de pago a diversas Cajas de Ahorro. Posteriormente estas cantidades eran retiradas en persona por la propia procesada o por alguna otra persona concertada con ella.

P.A.P. fue condenada por la Audiencia de instancia como autora responsable de los delitos de falsedad en documento público y malversación de caudales públicos, sin la concurrencia de circunstancias modificativas, apenas de privación de libertad, inhabilitación absoluta durante el mismo tiempo de la pena privativa de libertad y penas pecuniarias. Por otra parte la segunda procesada en esta misma causa P.P.G. fue condenada como autora responsable de los delitos de estafa y falsedad en documento oficial.

Se trata, como la misma sentencia de instancia reconoce y corrobora posteriormente el Tribunal Supremo, de delitos cometidos por medios informáticos en los que la utilización de la informática se constituye como elemento fundamental e imprescindible para la ejecución. No ofrece duda por

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

tanto el reconocimiento de la intervención del elemento informático en la comisión de los hechos delictivos. Tampoco ofrece duda el aprovechamiento por parte de P.A.P. de su destino en el departamento en que se producían o determinaban las altas en la prestación por desempleo. Se repite aquí la circunstancia de la concurrencia de una relación especial que facilita la comisión de los hechos. Relación especial que es aprovechada por la delincuente para facilitar la ejecución. De este modo los hechos cometidos por esta procesada no son calificados como de estafa sino como de malversación de caudales públicos, figura jurídica más cercana al fraude que a la estafa. Por el contrario los hechos cometidos por la segunda encausada P.P.G. son constitutivos de un delito de estafa, pues esta segunda encartada no disfruta de la relación especial de la primera. En definitiva fraude o estafa la concurrencia de la informática crea nuevos tipos penales.

Para mayor abundamiento puede ser citada la Sentencia de **5 de diciembre de 1989** en la que se reprueba una conducta que reúne todas las características del fraude informático: hay una manipulación del proceso informático, ánimo de lucro y perjuicio para tercero. En esta sentencia los dos procesados, un funcionario de la Seguridad Social y el propietario de un bar-restaurante, convienen que el funcionario lleve a cabo una serie de modificaciones en los datos de afiliación a la Seguridad Social de sus empleados de tal modo que se hacía variar la realidad en el ordenador variando la fecha del alta de distintas personas, todas ellas relacionadas laboralmente con uno de los procesados.

* **Referencia a jurisprudencia menor en relación con el uso abusivo de medios de pago**

Se recoge a continuación la jurisprudencia más reciente de las Audiencias Provinciales en relación con el uso de tarjetas electrónicas. La mayoría de la jurisprudencia que se analiza pertenece al orden civil aunque en muchos casos los hechos que dan origen al proceso civil son claramente delictivos, pero no se conoce al autor de los mismos.

Merecen especial detención las recientes declaraciones jurisprudenciales de nuestras Audiencias en las que siguiendo un criterio rector básico en derecho como son los dictados de la buena lógica arrojan luz sobre el conjunto de derechos y obligaciones que derivan de las relaciones contractuales entre

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

titulares, entidad emisora-gestora de la tarjeta y establecimientos adheridos al sistema.

No ofrece duda la implantación de las tarjetas de crédito en la práctica mercantil como sistema de pago. En gran medida esta realidad obedece a la aparición de nuevas tecnologías y a las exigencias modernas de mayor comodidad y seguridad en los pagos de las mercancías sin la necesidad de manipulación de numerario, expedición de talones bancarios o libramiento de letras de cambio. Si esto es una realidad incontestable no es menos cierto que esa mayor comodidad y seguridad en los pagos se ve acompañada por no pocas incidencias de las que ya han conocido nuestros Tribunales.

Se analiza a continuación la visión jurisprudencial en relación con la naturaleza jurídica de las tarjetas de crédito y dentro del ámbito de la responsabilidad civil los derechos, obligaciones y cargas del titular y del emisor de tarjetas de crédito y, en su caso, de los establecimientos adheridos al sistema.

Ya en 1976 el Tribunal Supremo determinó que las tarjetas electrónicas de pago tienen una naturaleza jurídica análoga a la de los títulos valores al concurrir la característica de la incorporación de un derecho a un título. Siendo, así mismo, este título personalísimo e intransferible. E consideración de la tarjeta como un título valor no excluye su caracterizaci... como un instrumento que la propia jurisprudencia califica de legitimación. La configuración de estos instrumentos de legitimación como verdaderos instrumentos de identificación de su titular sería una reivindicación que junto a equilibrar las posiciones evitaría el uso delictivo de estos instrumentos. La tarjeta se emite a nombre de una persona y esa persona es la única autorizada para hacer uso de ella. Sin embargo, siendo esta intransferibilidad del instrumento de pago una característica esencial del mismo, no se encuentra acompañada por un sistema de identificación que desde el punto de vista físico y lógico excluya la utilización de la tarjeta como medio de pago por un tercero no titular. Así pues, actualmente el que solamente sea el titular el autorizado para utilizar el instrumento de pago es una circunstancia que no deriva directamente de dicho instrumento sino de la naturaleza jurídica de la tarjeta y de la relación contractual subyacente.

* **Robo o pérdida de la tarjeta**

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Es en relación a este supuesto fáctico sobre el que se concentran mayor número de sentencias. Destacaremos ahora dos, una de **31 de enero de 1995** de la **Audiencia Provincial de Sevilla** y otra de **14 de mayo de 1993** de la **Audiencia Provincial de Barcelona**. En ambas sentencias el demandante es el establecimiento emisor (grandes almacenes) que reclama al titular de una tarjeta de compra las cantidades procedentes de las mercancías adquiridas por un tercero que utilizó la tarjeta de compra extraviada. Ambas sentencias establecen sobre el titular de la tarjeta una carga consistente en la guarda y custodia de la misma y de un deber inexcusable de notificación del extravío o robo. Cuestiones estas fundamentales ya que si el titular demuestra la debida diligencia en la custodia y conservación de la tarjeta, la sentencia de la Audiencia Provincial de Sevilla entiende que las tarjetas de crédito son asimilables a los cheques o títulos al portador viniendo en aplicación lo dispuesto en el artículo 156[77] de la Ley Cambiaria y del Cheque de 16 de julio de 1985. El citado precepto establece la responsabilidad civil del Banco o entidad financiera en los casos de pérdida o extravío de cheques que sería aplicable a la derivada de la pérdida o extravío de las tarjetas sobre la entidad expendedora.

Por su parte la Audiencia Provincial de Barcelona hace un análisis altamente esclarecedor de lo que ha de considerarse indiligente custodia de la tarjeta de crédito por parte de su titular. Para esta Audiencia es indiligente aquel titular que omitió en la guarda de la tarjeta no ya medidas de actuación de carácter excepcional, sino sencillamente la diligencia que correspondía a las circunstancias de las personas, del tiempo y del lugar conforme prevé el artículo 1.104[78] del Código civil, es decir, la diligencia que correspondería a

[77] Artículo 156 de la Ley 19/1985, de 16 de julio, Cambiaria y del Cheque:
"El daño que resulte del pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido negligente en la custodia del talonario de cheques, o hubiere procedido con culpa".

[78] Artículo 1.104 del Código civil:
"La culpa o negligencia del deudor consiste en la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar.
Cuando la obligación no exprese la diligencia que ha de prestarse en su cumplimiento, se exigirá la que correspondería a un buen padre de familia".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

un buen padre de familia. Cabría preguntarse cómo concretar esa diligencia del buen padre de familia en lo que respecta a la comunicación del extravío o robo de la tarjeta. Entendemos que para concretar esta diligencia del buen padre de familia son adecuados criterios interpretativos los siguientes: artículo 5 del primer proyecto de artículos (1986) previo a la Recomendación 88/590/CEE donde se afirma que el titular debe avisar al emisor dentro de las 48 horas siguientes a la CONSTATACION del robo, pérdida, etc. Así mismo en Estados Unidos la *Electronic Transfer Act* (1978) y la *Regulation E* (1980) consideran diligente la notificación a la entidad financiera emisora dentro de los dos días hábiles siguientes a tener conocimiento de la pérdida o robo. El problema radicaría en establecer el momento en que el titular conoce la pérdida o robo. La legislación norteamericana en este caso hace recaer sobre la entidad emisora la carga de demostrar que un titular conocía la pérdida o robo y que si hubiera notificado antes estos hechos se habrían evitado las pérdidas económicas que la entidad pretende imputar al titular. Indudablemente estos sistemas de reparto de responsabilidad parten del desconocimiento del autor material de las disposiciones, puesto que si éste es conocido él será el civil y criminalmente responsable.

* **Diligencia exigible al establecimiento-emisor**

Si la diligencia exigible al titular-consumidor parece no ofrecer dudas a nuestros Tribunales no se puede decir lo mismo de la que cabe exigir de los establecimientos sean o no emisores. Así debemos hacer notar la falta de unidad de criterio que presentan las dos sentencias de las Audiencias de Sevilla y Barcelona en relación con el contenido del deber de diligencia que corresponde al establecimiento emisor de la tarjeta (grandes almacenes) en la comprobación de las firmas e identidades de los usuarios de la tarjeta. Si para la Audiencia Provincial de Sevilla no puede obligarse a los empleados del establecimiento emisor a que procedan a la identificación mediante la exhibición del Documento Nacional de Identidad de todos y cada uno de los reales compradores de las mercancías o artículos vendidos, para la Audiencia de Barcelona es determinante de concurrencia de culpa en el establecimiento emisor de la tarjeta la no comprobación de la identidad del usuario de ésta. Divergencia que determina un fallo sustancialmente diverso en ambas sentencias ya que en la Sentencia de la Audiencia Provincial de Barcelona viene en aplicación la doctrina jurisprudencial de la compensación de culpas

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

quedando reducida a la mitad la cantidad reclamada por el establecimiento accionante, siendo sin embargo estimada en su totalidad la cantidad reclamada por éste en la sentencia de la Audiencia de Sevilla.

* **Extractos periódicos enviados por la entidad**

Si hasta aquí hemos analizado las recíprocas obligaciones en caso de robo o extravío debemos ahora detenernos en las recíprocas obligaciones en el desarrollo habitual de la cuenta de crédito asociada a la tarjeta. La **Audiencia Provincial de Alicante** en **sentencia de 12 de julio de 1994** determinó con claridad que es obligación de la entidad de crédito aportar los documentos acreditativos de los cargos y adeudos. De forma que el saldo deudor no puede entenderse debidamente justificado por la simple certificación unilateral de la entidad. Por otra parte corresponde al titular de la tarjeta la carga de impugnar las partidas concretas con las que discrepe ya que en caso contrario se estiman tácitamente aceptadas las partidas periódicamente enviadas por la entidad al titular (sentencia de la **Audiencia Provincial de Pontevedra de 27 de marzo de 1995**). ¿En qué plazo debe el titular de la tarjeta expresar puntualmente los reparos que tuviere contra los extractos? para la **Audiencia Provincial de Ciudad Real** en sentencia de **20 de mayo de 1993** transcurrido el plazo de dos meses se reputará tácitamente prestada la conformidad.

Siguiendo con el análisis de la Jurisprudencia más reciente en torno a las tarjetas electrónicas ahora nos detenemos en algunos aspectos que se desarrollan con habitualidad en la relación entidad-cliente (uso de la tarjeta en cajeros, renovación, cancelación) y que revisten una importancia máxima a la hora de distribuir las cuotas de responsabilidad ante una incidencia derivada del desarrollo de la relación contractual.

* **Identificación**

En la operativa habitual con tarjeta se produce una sucesión de hechos que aunque no reparemos en su trascendencia jurídica los Tribunales ya han analizado y precisado las responsabilidades derivadas de los mismos. Para muchos nos resulta habitual y hasta intranscendente acercarnos a un cajero automático con nuestra tarjeta, teclear un número y obtener dinero. Pues bien, aquí se plantea un conflictivo asunto como es el de la comprobación de nuestra

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

identidad. Alguna Sentencia ha afirmado que el emisor de la tarjeta no comprueba dicha identidad, sin embargo, paradójicamente dicha Sentencia no deriva responsabilidad alguna para la entidad por ello. En este punto la Ley 7/96, de Ordenación del Comercio Minorista de 17 de enero de 1996, al regular en su artículo 46[79] el pago mediante tarjeta de crédito en ventas a distancia utiliza un concepto "compra **efectivamente realizada por el titular** de la tarjeta" que deja traslucir el principio subyacente en dicho precepto, cual es la exigencia de acreditación de que una operación ha sido efectivamente realizada por el titular de la tarjeta. El legislador, por tanto, atribuye responsabilidad al titular en un cargo hecho con su tarjeta si, y solo si, "efectivamente" queda acreditado que el titular ha realizado dicho cargo. No habla este artículo 46 de desarrollo de la operación de compra regularmente con arreglo al sistema implementado por el emisor de la tarjeta, sino que profundiza más utilizando el adverbio "efectivamente" que transciende la propia y simple regularidad en el funcionamiento del sistema para adentrarse en el ámbito subjetivo y personal del que en realidad ha llevado a cabo una operación. Esta reciente regulación creemos es fundamental como nuevo criterio para la atribución de responsabilidad al titular en usos de su tarjeta, sólo si "efectivamente" se acredita que el titular hizo uso de la tarjeta será responsable civil criminalmente, según las circunstancias.

* **Renovación tarjeta**

Es frecuente recibir por correo ordinario o certificado la renovación de nuestra

[79] Ley 7/1996 de Ordenación del Comercio Minorista.
Artículo 46. Pago mediante tarjeta de crédito.-
"*1. Cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que ésta hubiese sido presentada directamente o identificada electrónicamente, su titular podrá exigir la inmediata anulación del cargo.*
En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad.
2. Sin embargo, si la compra hubiese sido efectivamente realizada por el titular de la tarjeta y, por lo tanto, hubiese exigido indebidamente la anulación del correspondiente cargo, aquél quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

tarjeta. Pues bien, según una sentencia de **9 de septiembre de 1994 de la Audiencia Provincial de Málaga** llegado el plazo de validez de una tarjeta la entidad emisora puede proceder a la renovación unilateral de la misma siempre que se observen unos determinados requisitos: 1º debe quedar acreditada la recepción de la nueva tarjeta por el titular. 2º Se considera un comportamiento indiligente por parte de la entidad el poner a disposición de uno de sus empleados la clave de identificación y la tarjeta renovada para que sean entregados a su titular.

En este mismo sentido el Juzgado Nueve bis de Madrid se pronunció favorablemente estimando la demanda y atribuyendo responsabilidad a la entidad emisora en disposiciones no autorizadas, al no quedar acreditada la recepción de la tarjeta por el titular, hecho cuya acreditación extinguiría dicha responsabilidad.

Según la citada doctrina jurisprudencial la distribución de las tarjetas renovadas debería efectuarse a través de un medio que dejara constancia de su recepción por el titular, como por ejemplo entrega en mano en la sucursal y firma del correspondiente recibí, o bien, correo certificado con acuse de recibo y contenido. Hemos apuntado una posible solución al problema de la acreditación de la entrega de la tarjeta renovada pero restaría por resolver el de la distribución del PIN. Esta entrega ha de ser confidencial y, conforme apunta la sentencia de la Audiencia de Málaga, es indiligente la puesta a disposición de los empleados de la entidad de estas claves secretas. A este respecto resulta interesante constatar el funcionamiento en algunas entidades de sistemas de generación y distribución automática de claves PIN para tarjetas. Los PIN generados con arreglo a este sistema no se guardan en ningún medio ni físico (papel) ni lógico (memoria del ordenador) y se distribuyen de forma confidencial a sus destinatarios.

En definitiva lo que se pretende es evitar supuestos fácticos como el conocido por la **Sala segunda del Tribunal Supremo en Sentencia de 8 de junio de 1995**. Los hechos son los siguientes: un funcionario de correos viola la correspondencia y apoderándose de las tarjetas de crédito que los bancos y cajas remiten por carta obtiene mediante engaño a sus titulares el PIN o número secreto. En esta Sentencia el Tribunal Supremo consideró responsable en grado de autoría de un **delito de infidelidad en la custodia de documentos**

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

y otro de **robo** al funcionario de correos. Habiéndose ejecutado los hechos merced al desempeño de las funciones encomendadas por su principal -el Estado- al funcionario infiel, se considera responsable civil subsidiario al Estado por los daños y perjuicios ocasionados. El Tribunal, sin embargo, no aprecia responsabilidad alguna en las entidades emisoras que remitieron por correo las tarjetas substraídas aunque ciertamente, y siguiendo la teoría de la causalidad, los hechos no habrían tenido lugar si el envío de las tarjetas no se hubiera efectuado por correo. Como reiteradamente ha puesto de manifiesto el Servicio de Reclamaciones del Banco de España al remitir por correo ordinario un instrumento cuya posesión por terceras personas puede dar lugar a disposiciones de fondos no autorizadas se origina un riesgo previsible y evitable de cuyas consecuencias dañosas debe responder la entidad.

* **Cancelación tarjeta**

El **Tribunal Supremo** conoció en **Sentencia de 15 de noviembre de 1994** de un supuesto de cancelación por una entidad de tarjeta de crédito sin justa causa. Los hechos se concretan en la cancelación de una tarjeta por error, que impide a su titular verse amparado por una póliza de seguro, a favor de todos los titulares de dicha tarjeta de crédito, por los daños corporales sufridos como consecuencia de los accidentes ocurridos en calidad de pasajeros en un medio de transporte público siempre que el importe del transporte hubiera sido pagado con la referida tarjeta de crédito. La responsabilidad de la entidad por la cancelación injustificada se cuantifica en el importe del premio de la póliza al haberse producido el óbito del titular de la tarjeta cancelada por accidente en el transcurso del viaje cuyo billete intentó adquirir con la mencionada tarjeta. El Tribunal Supremo en esta Sentencia establece dos obligaciones básicas a cargo de la entidad emisora de la tarjeta: 1ª comunicación previa al titular de la cancelación de su tarjeta siendo los efectos de esta cancelación siempre posteriores a dicha comunicación, y 2ª la entidad no puede proceder a la cancelación de una tarjeta de crédito de manera estrictamente arbitraria o caprichosa sino que necesariamente ha de concurrir una causa que la justifique. El Supremo lleva a cabo estas apreciaciones a pesar de encontrarse expresamente pactado, en el contrato que unía a entidad emisora de la tarjeta y titular fallecido, que aquélla se reservaba la facultad de cancelar la tarjeta durante su vigencia. Esta facultad de cancelación unilateral encontraba su origen en lo que fue una cláusula de estilo en muchos de los contratos entre

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

entidades emisoras-gestoras y titulares donde expresamente se decía que la entidad se reservaba el derecho de propiedad sobre la tarjeta. Todavía hoy algún contrato (Visa electrón de Caja Postal, Visa de BNP España, S.A., Visa electrón del Banco Exterior de España) recoge esta cláusula de reserva de propiedad, que puede encubrir una facultad abusiva de cancelación de la tarjeta injustificada, en cualquier momento y sin preaviso por parte de la entidad emisora-gestora. En este punto es clara nuestra ley para la Defensa de los Consumidores y Usuarios[80] al considerar contrarias a la buena fe y al justo equilibrio de las contraprestaciones las cláusulas que otorguen a una de las partes la facultad de resolver discrecionalmente el contrato. Esta interpretación sobre la intención subrepticia de algunas entidades al calificarse como propietarias de la tarjeta obligaría a sostener que el titular es un arrendatario o un comodatario. Sin embargo lo que justifica la devolución de la tarjeta al emisor no es ese supuesto derecho de propiedad sino la relación obligatoria de carácter crediticio entidad-cliente que cuando se extingue, justificadamente, obliga al extitular a devolver el instrumento que representaba dicho crédito. En definitiva la calificación como propietaria a la entidad emisora no encuentra adecuado acomodo jurídico en la compleja relación contractual entidad emisora-titular no pudiendo en ningún modo servir de fundamento, según la jurisprudencia analizada, a una cancelación unilateral e injustificada del instrumento de crédito (tarjeta).

Hasta aquí el repaso de la Jurisprudencia española más relevante sobre uso abusivo de sistemas y medios de tratamiento automático de la información. Cabría extraer como conclusión la escasez de sentencias en el orden penal y la reconducción de conductas indudablemente delictivas a otros órdenes como por

[80] Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.
Artículo 10.1."*Las cláusulas, condiciones o estipulaciones que, con carácter general, se apliquen a la oferta, promoción o venta de productos o servicios, incluidos los que faciliten las Administraciones públicas y las Entidades y Empresas de ellas dependientes, deberán cumplir los siguientes requisitos:*
(...)
c) Buena fe y justo equilibrio de las contraprestaciones, lo que, entre otras cosas, excluye:
(...)
2° Las cláusulas que otorguen a una de las partes la facultad de resolver discrecionalmente el contrato (...)".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ejemplo el civil.

2.3. CONCEPTO EN LA NORMATIVA SUPRANACIONAL

2.3.1. PROYECTO DE GUÍA JURÍDICA SOBRE LAS TRANSFERENCIAS ELECTRÓNICAS DE FONDOS: INFORME DEL SECRETARIO GENERAL DE LA CNUDMI

Aunque no son abundantes los estudios legales sobre la figura del fraude informático, destacaremos aquí los trabajos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en relación al fraude en las transferencias electrónicas de fondos. Así mismo merece estudio detallado la Recomendación del Consejo de Europa R(89)9 sobre Criminalidad Informática. Comenzaremos por el **"Proyecto de guía jurídica sobre las transferencias electrónicas de fondos: informe del Secretario General" de la CNUDMI**[81]. El tema del fraude informático es abordado en este Proyecto de guía jurídica en su faceta de fraude en la transmisión de los datos a distancia. En concreto se estudian las transferencias electrónicas de fondos y las pérdidas sufridas a consecuencia del fraude. Comienza advirtiendo la potencial gravedad que pueden revestir las acciones fraudulentas relacionadas con la transferencia electrónica de fondos. El volumen de las transferencias electrónicas de fondos y las sumas de dinero manejadas indican que las pérdidas potenciales pueden rebasar ampliamente las que se observan en las transferencias documentadas de fondos. De la constatación de esta realidad se deriva la preocupación de los clientes de los bancos de que la progresiva sustitución de las transferencias documentadas por las transferencias electrónicas de fondos, suponga la necesidad de asumir un mayor nivel de responsabilidad por las pérdidas producidas por error o por fraude.

A esta misma realidad hace referencia Kozolchyk[82] al ocuparse de las nuevas prácticas bancarias. Las comunicaciones entre bancos dejan de ser documentales

[81] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Proyecto de guía jurídica sobre las transferencias de fondos: informe del Secretario General*. Anuario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Vol. XV: 1984. Documento A/CN.9/250 add.4.

[82] KOZOLCHYK, Boris. *"Cartas de crédito electrónicas"*. En Revista de Derecho de los Negocios. Año 3, Número 22/23 Julio-Agosto 1992. Publica Editorial La Ley. Pág. 5 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

para convertirse en electrónicas. Como pone de manifiesto este autor es creciente el número de cartas de crédito que se comunican directamente por el emisor al ordenador del beneficiario a través de una red de telecomunicación. El uso de estos sistemas de telecomunicación hace necesario determinar la responsabilidad de la red de telecomunicaciones y de sus usuarios por funcionamiento o uso mal intencionado o negligente de la red. La red SWIFT puesta en funcionamiento por la Sociedad del mismo nombre, la SWIFT (*The Society for Worldwide Interbank Financial Telecommunications,* la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales), ha desarrollado procedimientos estándar para la formulación y tramitación de negociaciones y pagos de créditos por medios electrónicos a través de esta red. Un mensaje interbancario que circule por la red SWIFT describe el siguiente recorrido: el mensaje tiene su origen en un usuario de la red, se transmite al Punto de Acceso SWIFT (SAP) más cercano. Desde el SAP el mensaje se dirige al Procesador Regional (RP) allí se valida el mensaje. A continuación el mensaje se encamina a los centros principales de conmutación o Centros Operativos (OC). Desde el OC el mensaje describe el camino inverso hasta llegar al ordenador del banco receptor. De acuerdo con nuestros datos la red SWIFT tiene dos centros operativos uno en los Países Bajos y otro en Estados Unidos. Los mensajes que se transmiten a los OC se transmiten a través de líneas dedicadas propias de la SWIFT. Lo realmente destacable de esta red y la razón por la que se menciona en este punto es la exigencia de normalización de todos los mensajes que por ella se transportan. Así mismo las estrictas medidas de seguridad adoptadas en la red permiten tener certeza de que el mensaje recibido es el mismo que envió el emisor. Junto a estos temas se plantea el fundamental de la responsabilidad. Responsabilidad que tanto puede venir derivada de negligencia y dolo como de la demora en la transmisión de un mensaje. En principio en la red SWIFT la responsabilidad se establece por la culpa. Pero en la práctica los riesgos de una transmisión negligente o dolosa se comparten entre SWIFT y los usuarios. El sistema de distribución de la responsabilidad en SWIFT se basa en un principio fundamental: "SWIFT no es responsable por ningún segmento de la teletransmisión que no esté directamente bajo su control"[83]. De acuerdo con esto es la Sociedad para las Telecomunicaciones Interbancarias Mundiales, la encargada de mantener los niveles adecuados de seguridad en la parte de red que controla. Ahora bien de lo que ya no es responsable la SWIFT es de la seguridad de las instalaciones de comunicaciones, de las líneas dedicadas o de las propias

[83] KOZOLCHYK, Boris. Op. Cit. Pág. 10.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

instalaciones informáticas de los bancos usuarios. Junto a ese principio general antes apuntado de la exclusión de la responsabilidad de la SWIFT en todos aquellos segmentos de la teletransmisión sobre los que no tenga control directo se deben tener en cuenta otros principios adyacentes: 1º. La Sociedad para las Telecomunicaciones Interbancarias Mundiales no es responsable de las pérdidas producidas por fallos técnicos o por causa de fuerza mayor. 2º. Tampoco es responsable la Sociedad por haber dado curso a una operación no autorizada, salvo que el perjudicado demuestre que SWIFT podía haber supuesto que el mensaje no estaba autorizado. 3º. La SWIFT puede servirse de un tercero para la transmisión siempre que se respeten las garantías de seguridad generales ofrecidas por la red . 4º. La SWIFT nunca es responsable por las negligencias cometidas por el usuario. 5º. Si se demuestra la negligencia de SWIFT o el dolo de alguno de sus empleados, sólo se responsabiliza de las pérdidas directas de los usuarios. Por pérdida directa se entiende una pérdida irrecuperable de fondos correspondientes al principal de una operación bancaria y a los intereses producidos por el principal. Junto a esta delimitación del concepto de pérdida directa la SWIFT establece una limitación cuantitativa de su responsabilidad. De este modo si las pérdidas directas se han producido por actos dolosos o fraudulentos de empleados de la SWIFT, ésta no responde por una suma superior a tres millones de francos belgas para una sola pérdida o para una serie de pérdidas ocasionadas por un mismo acto doloso o fraudulento. La cantidad de la que se hace responsable la SWIFT por pérdidas en estos conceptos no puede superar los seis millones de francos belgas para cada período anual. Ante este tipo de limitaciones se puede presentar el caso de que las responsabilidades de la SWIFT por actos dolosos o fraudulentos de sus empleados supere los límites cuantitativos antes indicados, en estos casos la indemnización máxima anual disponible se repartirá entre los reclamantes en función de los daños sufridos por éstos. Este tipo de cláusulas que establecen una responsabilidad rígida de carácter cuantitativo, independientemente de la cuantía de la operación en cuestión, son completamente nulas en derecho español de acuerdo con la ley General para la protección de los consumidores y usuarios[84].

Hasta ahora se han mencionado supuestos de responsabilidad por negligencia y dolo, pero también se prevén por las reglas SWIFT los supuestos de responsabilidad por demora. Las situaciones de hecho a las que se intenta poner

[84] Ley de 19 de julio de 1984, núm. 26/1984. BOE de 24 de julio de 1984, núm. 176, pág. 21686.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

remedio en estos casos serían todas aquéllas en las que se produce una demora en la emisión o en la retransmisión de una instrucción de transferir fondos. Estos retrasos provocan pérdidas de intereses a favor del transmitente o intereses en su contra si lo que se retrasa es la solución de un débito. La SWIFT de acuerdo con las normas que tiene aprobadas se hace responsable por estas pérdidas en los siguientes casos: 1°. Si el mensaje del emisor reconocido por éste no aparece en el informe de mensajes sin entregar y no es entregado. 2°. Cuando la SWIFT no notifica de un fallo del personal de la SWIFT. 3°. Cuando la SWIFT no notifica de un fallo en la red. Las reglas para el establecimiento de la responsabilidad del emisor son las siguientes: 1°. El mensaje no es reconocido por SWIFT y sin embargo el emisor no inicia el procedimiento adecuado para que se produzca tal reconocimiento. 2°. El mensaje del emisor fue reconocido pero luego apareció en el informe de Mensajes sin Entregar. 3°. Una transmisión que requería un formato SWIFT es transmitida con otro formato. 4°. El emisor no reacciona con prontitud, y sigue enviando mensajes, ante el aviso de SWIFT de que un elemento de la red funciona defectuosamente. 5°. El mensaje contenía una dirección inválida en la cabecera o en el texto.

Por último se establecen los criterios de responsabilidad del receptor del mensaje por demora. 1°. El primer criterio para la atribución de responsabilidad se basa en una falta de adecuado tratamiento de mensajes con direcciones válidas recibidos antes del tiempo de desconexión de la red. 2°. No reaccionar con prontitud a las indicaciones de SWIFT sobre uso del sistema. 3°. No ajustarse a todas las reglas del sistema de forma que se asegure la recepción de todos los mensajes. 4°. No ajustarse a las reglas establecidas por la SWIFT sobre terminales informáticos, o bien, no haber notificado con veinticuatro horas de antelación de las circunstancias que le impiden adherirse a estas reglas. 5°. No seguir las prácticas bancarias habituales.

En resumen como se puede ver las reglas de la SWIFT reparten la responsabilidad entre el portador, en este caso la SWIFT, los bancos emisor y receptor, usuarios del servicio, y, en caso de existir, los respectivos aseguradores. Para Kozolchyk se aprecia en estas reglas un paralelismo con las leyes de principios de siglo para el reparto de la responsabilidad por riesgo en el transporte marítimo. En cualquier caso se aprecia en los criterios de reparto de la responsabilidad la

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

finalidad de no atribuir a la SWIFT la responsabilidad de toda pérdida, sino más bien al contrario, si todos los participantes en la red están interesados en que llegue a feliz término el transporte del mensaje, todos deben soportar su cuota de responsabilidad. Estas consideraciones a las que se llega con el estudio de las reglas SWIFT deben ser completadas con las establecidas por la **Comisión para el Derecho Mercantil Internacional de las Naciones Unidas.**

La continua evolución tecnológica hace realmente más difícil precisar con exactitud las cuotas de responsabilidad de cada uno de los sujetos intervinientes en este tipo de transferencias. Resulta complicado establecer estas cuotas de responsabilidad de las partes intervinientes en una transferencia de fondos, porque lo primero que resulta harto difícil es aplicar a las transferencias electrónicas de fondos las normas sobre responsabilidad propias de las transferencias documentadas. Como decíamos antes el problema se agudiza por la continua evolución del sector de las telecomunicaciones. No debemos olvidar que es cada vez más frecuente la utilización de una red en el procesamiento y almacenamiento de datos. La información que se encuentra en estado de transmisión es sin duda la que sufre un mayor nivel de vulnerabilidad. La utilización de esta red se configura como una red punto a punto que vincula distintas sucursales mediante líneas dedicadas especiales. Las telecomunicaciones eran antes un servicio ajeno al Banco que se ofrecía por una empresa de telecomunicaciones en régimen monopolístico. Hoy ya no es así, los sistemas de telecomunicaciones utilizados por los Bancos son redes alquiladas, no ya siempre a una única empresa que monopoliza el sector, sino a aquella que ofrece las mejores condiciones para el Banco. De la constatación de esta realidad se deduce la falta de fundamento de la exención de responsabilidad de los servicios de telecomunicaciones ante una situación de fraude o de error en una transferencia electrónica de fondos. Se estudiarán a partir de este momento las **conductas fraudulentas realizadas en la teletransmisión de los datos**. De acuerdo, por tanto, con la clasificación del Prof. Davara[85] de los tipos de manipulación de datos se atenderá , a partir de ahora, a la cuarta de estas clasificaciones: manipulación de los datos en la transmisión de los resultados del proceso.

Pasando al análisis del **fraude en las transferencias electrónicas de fondos**, y de los criterios de reparto de las responsabilidades que de él derivan, el **documento**

[85] DAVARA RODRIGUEZ, Miguel Angel. Op. Cit. Pág. 324.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de Naciones Unidas recoge las siguientes fuentes u orígenes del mismo: prácticas deshonestas de los empleados del cliente del banco, uso fraudulento de terminales activados por los clientes, órdenes legibles por la máquina que suministra el cliente, fraude cometido por empleados del banco y fraude mediante la intervención en transmisiones de telecomunicaciones. **El fraude contemplado en este documento se limita al sector bancario** continuando tras la exposición de estas formas de fraude con el estudio del tratamiento jurídico que debe darse a una orden fraudulenta de débito en una cuenta, los sistemas de prevención del fraude, y por último, la responsabilidad del banco originario ante su cliente por errores o fraudes cometidos en una transferencia interbancaria.

En relación con el primer punto referente a las formas de fraude, en las prácticas deshonestas de los empleados del cliente del banco, se pueden describir tres formas o ejemplos típicos de deshonestidad en los empleados de clientes de un banco. 1°. El empleado encargado de preparar la nómina de pagos o los comprobantes en que se autoriza el pago a un proveedor falsifica cualquiera de ambos documentos, de modo que el pago se hace a una persona no facultada para recibirlo. La forma de pago es indistinta, bien se trate de un pago efectuado por cheque o bien se haga mediante transferencia documentada o electrónica los fondos siempre irán a parar a la cuenta de una persona ficticia. 2°. El empleado deshonesto está facultado para autorizar transferencias de fondos en nombre de su empleador. Lleva a cabo estas transferencias de fondos sin que respondan a negocios reales y consuma posteriormente el fraude retirando los fondos. En estos dos primeros casos de fraude la orden de transferencia de fondos aparece como válida ante el banco que la hará efectiva. La causa que la origina es sin embargo falsa, no existe en realidad. 3°. El tercer ejemplo más característico de prácticas fraudulentas de empleados de clientes de bancos es aquél en el que el cliente del banco dispone en su propia empresa o centro de trabajo de un terminal para llevar a cabo transferencias de fondos electrónicas. El empleado deshonesto tiene acceso al terminal y conoce el procedimiento para el envío de una orden de transferencia electrónica de fondos. Emite esta orden que automáticamente es ejecutada por el banco. Los tres ejemplos mencionados presentan matices diferentes. En el primero, el empleado falsifica la documentación probatoria de la transferencia de fondos fraudulenta, en el segundo, el empleado deshonesto autoriza operaciones inexistentes (firma cheques u órdenes de transferencia documentada de créditos o autoriza transmisiones electrónicas de fondos), en el tercer ejemplo presentado el empleado utiliza unos medios a los que no tiene legítimo acceso.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Aún se puede distinguir una cuarta modalidad general de fraude en aquellos ordenamientos que se reconoce validez jurídica a la firma electrónica[86]. La situación que se puede plantear sería aquélla en la que se presenta al banco una orden de transferencia de fondos firmada fraudulentamente. Si el banco al aceptar esta transferencia de fondos lo hace de buena fe[87] sin albergar sospecha sobre la legitimidad de la firma, puede debitar la cuenta de su cliente, aunque estemos ante una firma fraudulenta como ya hemos dicho. La razón para hacer soportar al cliente toda la carga de las consecuencias del fraude se fundamenta en el hecho de que al banco le es imposible distinguir entre el uso auténtico y el uso indebido del mecanismo de firma. Es el cliente del banco el que tiene la responsabilidad de vigilar que el mecanismo de firma electrónica es usado exclusivamente por las personas que están autorizadas para ello. Si el mecanismo de firma electrónica ha sido utilizado por una persona no autorizada lo que ha existido es una negligencia por parte del cliente del banco al no custodiar adecuadamente dicho mecanismo[88]. Los mismos argumentos utilizados para autorizar el débito en la cuenta del cliente por uso fraudulento de la firma electrónica, se podrían utilizar para hacer responder al cliente por el monto de una orden fraudulenta de transferencia de fondos realizada, utilizando un terminal de ordenador ubicado en el establecimiento del cliente. Sin embargo en estos casos, como señala el informe de la Comisión de las Naciones Unidas, se produce un reparto de la responsabilidad entre el cliente y el banco. Esto es así porque la responsabilidad del mantenimiento de la seguridad del terminal ubicado en el establecimiento del cliente es compartida entre banco y cliente.

---

[86] Nuestro ordenamiento jurídico cuenta ya con diversas normas que regulan el uso de la criptografía y, en concreto, la firma electrónica reconociéndole plena validez jurídica y eficacia probatoria. Cabe citar el Real Decreto 1369/1987 de 18 de septiembre, por el que se crea el Sistema Nacional de Compensación Electrónica; la Orden de 29 de febrero de 1988 sobre el Sistema Nacional de Compensación Electrónica.

[87] Previa comprobación de la identidad de los ordenantes.

[88] Confrontar con la Sentencia de 16 de julio de 1987 del Tribunal Supremo. En esta Sentencia y en relación con el delito de estafa se señala que si el perjuicio patrimonial se produce casualmente por la negligencia del sujeto pasivo o del perjudicado, que pueden ser distintos, el engaño se convierte en atípico y no puede ser sancionado. Por tanto, la falta de diligencia se configura como elemento destipificador y despenalizador del engaño. En un proceso de razonamiento paralelo el documento que se analiza imputa toda la responsabilidad al cliente del banco por su falta de diligencia en la custodia del mecanismo de firma electrónica.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Junto a este primer grupo de conductas fraudulentas englobadas bajo el epígrafe de prácticas deshonestas de los empleados del cliente de un banco, se distingue un segundo grupo de actos fraudulentos: el uso fraudulento de terminales activados por clientes.

La característica común de los terminales activados por el cliente es que en su uso no media intervención humana por parte del banco. Esto puede contribuir a aumentar las posibilidades de fraude. El procedimiento de autorización para el uso de estos terminales es determinado por el banco. El banco debe instalar el mejor sistema de seguridad teniendo en cuenta dos factores: el costo del sistema y las dificultades de su uso. El cliente en el uso del sistema de seguridad debe demostrar la suficiente diligencia en seguir las medidas establecidas.

El tercer grupo de conductas fraudulentas se engloban dentro de las prácticas de entrega por el cliente de órdenes directamente legibles por la máquina. Las situaciones que aquí se contemplan son aquéllas en las que el cliente suministra al banco o a una cámara de compensación, órdenes de transferencia de fondos en soporte directamente legible por un ordenador. Aquí es el banco o la cámara de compensación, los encargados de verificar dichos soportes antes de procesar las instrucciones y datos que contiene.

En cuarto lugar se pueden recoger todas aquellas conductas fraudulentas cometidas por empleados del mismo banco. A este tipo de conductas se refieren algunas de las sentencias estudiadas como doctrina jurisprudencial establecida por el Tribunal Supremo español en materia de fraude informático. En estos casos es un empleado deshonesto del banco el que programa la computadora para transferir indebidamente fondos a una cuenta por él controlada. La Comisión de las Naciones Unidas no hace referencia a otras prácticas igualmente fraudulentas por parte de empleados del banco, aunque sí apunta un tema de vital importancia para lograr el esclarecimiento de muchas de estas prácticas. Dice la Comisión que los ordenadores de los bancos deben ser programados de forma que se deje una constancia de todas las operaciones llevadas a cabo desde cualquier terminal del banco. Si no existe esta "pista de verificación completa de toda actividad", es relativamente fácil para el empleado defraudador ocultar su conducta engañosa, y

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

para el banco realmente difícil descubrirla[89].

Para terminar con esta relación de formas de fraude ha de mencionarse el fraude mediante la intervención de transmisiones de telecomunicaciones. Todo sistema de teletransmisión se ve sometido al riesgo de introducción de mensajes falsos en la línea de transmisión, la alteración de los mensajes legítimamente emitidos, interceptación de la línea, etc... En estos casos se enmarcarían las medidas de seguridad establecidas por la red SWIFT antes apuntadas.

Evitar todas estas intervenciones no autorizadas en las transmisiones supone adoptar medidas de seguridad en tres ámbitos fundamentales: el físico, el lógico y el jurídico. Al estudio más detenido de estos tres ámbitos de seguridad se dedican capítulos posteriores de este trabajo por lo que aquí únicamente baste una referencia a ellos. El documento de la Comisión de Naciones Unidas apunta como posible vía de solución, el establecimiento de un sistema que permita codificar la información teletransmitida. Junto a este sistema se apunta también la conveniencia de establecer un registro riguroso de toda orden de entrada o salida de transferencia de fondos. Asignando números secuenciales de entrada y salida a cada operación de transferencia de fondos, se puede detectar la existencia de una orden fraudulenta o que ha sufrido una manipulación al no corresponder los números de emisión y recepción o las horas en que dichas operaciones se efectuaron.

Se han expuesto hasta aquí aquellas formas de fraude que la Comisión de Naciones Unidas recoge en el documento que se viene analizando. La exposición aún no coincidiendo con la propuesta por parte de la doctrina[90] viene a aludir a las mismas fuentes de manipulación: la entrada de datos, el proceso de los datos, los datos intermedios, la salida y la transmisión de los datos.

---

[89] DAVARA RODRIGUEZ, en su obra *Derecho Informático,* analiza dentro de las características comunes a los delitos informáticos la "facilidad para encubrir el hecho" y la "facilidad para borrar las pruebas" en clara alusión al problema que aquí se apunta. De estas características específicas de los delitos informáticos deduce este autor "la necesidad de un tratamiento autónomo que estudie, en forma independiente de la rama del Derecho en la que se incluya, las acciones delictivas cometidas por medios informáticos ...., por sus particularidades y características realmente diferentes e independientes"

[90] DAVARA RODRIGUEZ, Miguel Angel. Op. Cit. Pág. 323 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Si interesante resulta conocer la tipología del fraude informático, no menos importante es estudiar las consecuencias de la ejecución de una orden fraudulenta de transferencia de fondos. En las reglas que a continuación se recogen como en las reglas de la SWIFT, ya vistas, también se establece un principio general de responsabilidad por culpa.

En principio no se puede debitar la cuenta de un cliente si la orden no está debidamente autorizada. Ahora bien si el débito se ha producido por la falta de controles adecuados por parte del cliente, debe soportar la carga del débito este cliente. El supuesto que se contempla es aquél en el que los empleados autorizados del cliente efectúan una transferencia fraudulenta, pero para el banco es una orden totalmente correcta efectuada por quien está autorizado para ello. El banco no puede advertir la existencia de ninguna anomalía en la operación, por tanto no puede hacérsele responsable de algo sobre lo que no tiene capacidad de control. Es por tanto el cliente el único responsable por su falta de diligencia en establecer los controles adecuados para evitar emisiones fraudulentas de órdenes de pago.

Sin embargo cuando la negligencia por parte del cliente del banco no sea tan fácil de establecer debe tenerse en cuenta una circunstancia fundamental: que "es el banco el que diseña los procedimientos básicos de seguridad y autorización"[91] en las transferencias electrónicas de fondos y el cliente el que los pone en práctica. Desde este planteamiento es adecuado adoptar unos criterios que permitan repartir la responsabilidad entre banco y cliente, ya que éste usa los sistemas que el banco pone a su alcance sin mediar negligencia por parte del cliente. Si el fraude se produce obedece a dos categorías de razones fundamentalmente: o bien ha existido una falta de diligencia por parte del cliente o bien los procedimientos de seguridad y autorización establecidos por el banco eran inadecuados. Pero en la mayoría de las ocasiones la determinación de si la orden fraudulenta responde a una o a otra de estas categorías no resulta fácil.

[91] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Proyecto de guía jurídica sobre las transferencias electrónicas de fondos: informe del secretario general de la CNUDMI. Capítulo VI sobre el fraude, los errores, la tramitación incorrecta de órdenes de transferencia y la responsabilidad consiguiente. &26.* Anuario de la CNUDMI Vol. XV: 1984. A/CN.9/250/Add.4.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Se debe tender a buscar fórmulas que sirvan para resolver la mayoría de los casos. En los contratos que ligan al cliente con su banco, la mayoría de ellos, facultan al banco para debitar en la cuenta del cliente cuando la operación se ha llevado a cabo mediante un terminal activado por el cliente utilizando su número de identificación personal o su palabra de paso. Este régimen cesa cuando el cliente pone en conocimiento del banco que su número de identificación personal o su palabra de paso le han sido substraídas. Por tanto la responsabilidad del cliente cesa en el momento que adopta las medidas necesarias para evitar la transferencia fraudulenta, mientras el funcionamiento del sistema es normal el riesgo de la transferencia fraudulenta lo soporta el cliente. En estos casos la atención se centra en el uso no autorizado de tarjetas con banda magnética. Es cierto que el uso no autorizado de este tipo de tarjetas puede constituir una forma de fraude informático, como ya se ha visto y en el capítulo siguiente se analizará, pero ahora nos interesa más centrar el tema de la responsabilidad por fraude en una transferencia en la que han tenido intervención además del cliente dos bancos. Se trata de transferencias interbancarias en las que además de la responsabilidad de los intervinientes en la transferencia, debe estudiarse la responsabilidad de la red de telecomunicación que soporta el transporte de los datos relativos a la transferencia.

Se contemplan en el documento de la CNUDMI[92] dos tipos de operaciones distintas: transferencias de débitos y transferencias de créditos, ambas hechas a distancia . En una transferencia de débitos intervienen: el banco depositario o adquirente, que recibe la orden de transferencia de fondos de su cliente; la parte originaria, que es la parte que presenta la orden de transferencia de fondos al banco originario; el banco destinatario que en realidad es el transmitente del débito. En las transferencias de créditos los papeles se invierten. El banco originario es banco transmitente del crédito y el banco destinatario es el adquirente de ese crédito. El enfoque de la cuestión se hace a través del establecimiento del paralelismo entre estas operaciones de transferencia electrónica de fondos y los contratos de transporte de mercancías por un porteador público. En el caso de estos últimos contratos el transporte de las mercancías requiere la intervención de distintos sujetos: agentes expedidores de carga, empresarios de terminal, transportistas de diverso tipo etc. Lo que se pretende es la obtención de

[92] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

un resultado: llevar la carga al punto de destino. La empresa con la que contrata el cliente el transporte de sus mercancías puede asumir la responsabilidad de garantizar el resultado del transporte, o bien simplemente asumir la responsabilidad de su parte de intervención en el porte acudiendo al agente mediador adecuado que pueda proseguir la ejecución del transporte. El supuesto de hecho que se contempla en las transferencias de fondos es muy similar. El cliente del banco originario quiere llevar a cabo una transferencia de fondos y proporciona al banco originario el nombre del banco destinatario de la transferencia, pero ninguna referencia se hace en relación a los medios de comunicación que se utilizarán entre los bancos, ni si intervendrán bancos intermediarios. Por tanto es el banco originario el que determina el conducto adecuado para efectuar la comunicación. Si este banco originario no asume la responsabilidad de responder por el buen término de la operación de transferencia iniciada, el cliente será el que en definitiva soportará la pérdida ante la práctica imposibilidad de demostrar dónde y por qué se produjo el fraude o el error en el transporte de los datos. Por eso la CNUDMI propone como más adecuado un sistema en el que el banco originario asuma la responsabilidad por la debida ejecución de la transferencia de fondos. Este sistema también debe prever algunas situaciones de exoneración de responsabilidad del banco originario. La CNUDMI recomienda así el traspaso de la responsabilidad por mal funcionamiento de la red, o por intervención fraudulenta de ésta al banco originario que en definitiva es el que elige esa red en concreto para ejecutar la transferencia ordenada por el cliente.

Más precisas son las reglas de la SWIFT, ya vistas, para la determinación de la responsabilidad por error o fraude en una transferencia interbancaria. En estas reglas impera el principio fundamental de la responsabilidad por culpa junto con el principio general de la exclusión de la responsabilidad de la SWIFT en todos aquellos segmentos de la teletransmisión sobre los que no tenga control directo.

El documento de la CNUDMI aborda a continuación un punto clave para la interpretación de las cláusulas de exoneración de responsabilidad en los contratos entre cliente, banco y entidades intermediarias en la transferencia de fondos. La solución a la que se llegue en este punto reviste máxima importancia en la interpretación de la posible solución de los conflictos que se planteen entre cliente del banco y la entidad financiera en los casos de fraude en la ejecución de una operación de transferencia de fondos. Para dar una visión acomodada al ordenamiento interno español deben tenerse en cuenta los siguientes textos legales:

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Constitución Española artículo 51, Ley General para la Defensa de los Consumidores y Usuarios[93] y la Propuesta Modificada de Directiva del Consejo *A la Protección de los Consumidores en Materia de Contratos Negociados a Distancia*, presentada por la Comisión de las Comunidades Europeas en Bruselas el 7 de octubre de 1993. Desde fecha reciente contamos en derecho español con una ley, la Ley 7/1996 de 17 de enero de 1996 de Ordenación del Comercio Minorista, que en su Título III ("Ventas especiales"), Capítulo II ("Ventas a distancia") recoge el régimen jurídico de las ventas celebradas sin presencia física simultánea del comprador y del vendedor en las que la contratación se realiza a través de un medio de comunicación a distancia. Esta ley puede calificarse de tuitiva respecto del consumidor en las transferencias electrónicas de fondos,[94] ya

[93] Ley 26/1984, de 19 de julio, publicada en el "Boletín Oficial del Estado" de 24 de julio, General para la Defensa de los Consumidores y Usuarios.

[94] Ya en **1985** el **Consejo de las Comunidades Europeas** aprobó una **Directiva referente a la protección de los consumidores en el caso de contratos negociados fuera de los establecimientos mercantiles**. Esta Directiva estableció un conjunto de medidas de protección del consumidor al entender que en los contratos que se celebran fuera del establecimiento del comerciante, concurren una serie de circunstancias, como la iniciativa de éste y la imposibilidad de comparación de la calidad y el precio de la oferta, que pueden derivar en prácticas comerciales abusivas.
Como norma de transposición a Derecho español se dictó la **ley 26/1991, de 21 de noviembre, de protección de los consumidores en el caso de contratos celabrados fuera de los establecimientos mercantiles**. Esta ley, en una interpretación extensiva, podría venir en aplicación a los contratos celebrados a través de medios informáticos y telemáticos. Si estos contratos se celebran fuera del establecimiento mercantil del empresario cabría argumentar quedan dentro del ámbito de aplicación de la susodicha ley. Sin embargo, no dejan de presentarse algunas dificultades para extender dicho ámbito de aplicación ya que esta ley exige el requisito formal de la documentación del contrato o de la oferta contractual por escrito e ir firmado "de puño y letra" por el consumidor. Exigencias que no se acomodan bien a la agilidad exigida en los contratos formalizados a través de teleinformática.
En todo caso, ya se apunta en la ley 26/1991 un derecho del consumidor al desistimiento del contrato que veremos es un derecho básico del comprador a distancia.
El legislador español consciente de los profundos cambios que ha experimentado la distribución comercial con la incorporación de las nuevas tecnologías recoge en la **ley 7/1996, de 17 de enero de Ordenación del Comercio Minorista**, un marco legal de mínimos, en torno al sistema de **ventas a distancia**. Es una ley con escasas referencias técnicas que busca establecer con claridad el citado marco legal coincidente con la posición europea en la materia expresada en la **Posición Común (CE) nº 19/95, aprobada por el Consejo**. Así en toda oferta de venta a distancia debe quedar identificado el proveedor, las características especiales del producto, el precio, debidamente separados los gastos de transporte, la

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

que en su artículo 46 en los supuestos de pago con tarjeta, en estas ventas a distancia, el titular puede exigir la inmediata anulación del cargo si el importe de la compra hubiere sido cargado utilizando el número de la tarjeta de crédito sin que ésta hubiere sido presentada directamente o identificada electrónicamente. Se puede deducir de los preceptos y leyes antes citados una protección, en derecho español y comunitario, del consumidor y usuario de servicios financieros, y en general frente al uso de las Tecnologías de la Información y las Comunicaciones en sus relaciones de derecho privado.

Las cláusulas de exoneración de responsabilidad normalmente se consignan en los contratos entre el banco originario y su cliente, entre los mismos bancos, entre las cámaras de compensación, los servicios de telecomunicaciones y otras partes que puedan intervenir en la transferencia de fondos. En este caso nos interesa especialmente las cláusulas de exoneración recogidas en los contratos entre cliente y banco. Estas cláusulas de exoneración pueden estipular que la parte exonerada no será responsable de la pérdida causada por terceros e incluso llegan a establecer la exoneración por actos u omisiones de la propia parte que se exonera. Esta última cláusula de dudosa legalidad habrá de interpretarse en consonancia con el artículo 1.902 del Código Civil[95]. El valor jurídico de estas cláusulas de

forma de pago y las modalidades de entrega o de ejecución y el plazo de validez de la oferta. Se prohíben los envíos no solicitados y se reconoce un derecho de desistimiento del comprador en los siete días contados desde la fecha de recepción del producto. Para evitar que esta legislación tuitiva, de los derechos del consumidor, pueda verse burlada si se designa como ley aplicable al contrato el Derecho de un país tercero que no reconoce tales derechos a los consumidores se arbitra una doble vía: por un lado la irrenunciabilidad de derechos y por otro que la ley a la que se hayan sometido las partes tenga alguna conexión con el negocio en cuestión.
En cuanto al pago mediante tarjeta en ventas a distancia el titular puede exigir la inmediata anulación de aquel cargo proveniente de una compra realizada utilizando el número de una tarjeta de crédito sin que ésta se haya presentado directamente o haya sido identificada electrónicamente. En estos casos, aunque no lo diga expresamente la ley, parece que la responsabilidad recae sobre el vendedor. Ahora bien si la compra ha sido efectivamente realizada por el titular de la tarjeta y ha exigido indebidamente la anulación del correspondiente cargo el comprador quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios.

[95] El artículo 1902 del Código Civil al establecer la denominada culpa extracontractual será aplicable en el caso de una culpa o dolo, excepcional o fuera de las coordenadas que enmarcan una actuación profesional. De forma que si el perjuicio o daño se produce dentro de la órbita de lo pactado por las partes vendrá en aplicación lo establecido por las partes en el contrato, pero a falta de pacto y si por causas

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ajenas al normal desarrollo surge una situación de hecho fuera del marco legal, debe entrar en juego el artículo 1.902 del Código Civil. Por tanto, no es suficiente que haya un contrato entre las partes para que la responsabilidad establecida en dicho contrato excluya la responsabilidad aquiliana o extracontractual del 1.902. Para que esta exclusión ocurra se requiere que el hecho dañoso se produzca dentro de la esfera de lo pactado. Por tanto, en las relaciones contractuales entre banco y cliente, Cámara de Compensación y banco, etc..., la existencia de una cláusula de exoneración de responsabilidad en el contrato será aceptable si el hecho se ha producido dentro de la órbita de lo pactado, si no vendrá en aplicación la responsabilidad extracontractual. Es decir la responsabilidad extracontractual también es aplicable, a tenor de lo expuesto, aunque exista contrato. Además ha de tenerse en cuenta que la responsabilidad extracontractual, aunque se basa en el elemento subjetivo de la culpabilidad, ha evolucionado en la jurisprudencia, sobre todo a partir de la Sentencia del Tribunal Supremo de 10 de julio de 1943, hacia un sistema cercano a la aceptación de situaciones cuasi-objetivas. Esta evolución jurisprudencial se ha hecho necesaria por el incremento de actividades peligrosas consiguientes al desarrollo de la técnica y el principio de ponerse a cargo de quien obtiene el provecho la indemnización del quebranto sufrido. En el caso de las transferencias electrónicas la utilización de los nuevos medios producen evidentes ventajas pero también pueden producir grandes pérdidas debido al altísimo volumen de operaciones que hoy se tramitan por medios electrónicos. Las evidentes ventajas de rapidez y comodidad que la utilización de los medios electrónicos comporta en la tramitación de las transferencias de fondos, debe conjugarse con una paralela responsabilidad por parte del banco o entidad financiera de garantizar el buen fin de la operación y de ahí se deduciría la atribución de la indemnización por el perjuicio ocasionado.

Por otra parte la jurisprudencia del Tribunal Supremo tiene reiteradamente declarado que la aplicación del artículo 1902 se hará no sólo en caso de omisión de normas inexcusables o aconsejadas por la más elemental experiencia, sino también ante un actuar no ajustado a la diligencia exigible según las circunstancias del caso concreto. Y se presumirá culposa toda acción u omisión que genere un daño indemnizable aunque se haya respetado la diligencia administrativamente reglada, pues la simple observancia de tales disposiciones no basta para exonerar de responsabilidad. Así mismo dice el Tribunal Supremo que no puede alegarse caso fortuito, como causa de exoneración de responsabilidad, cuando no se da la imprevisibilidad del suceso. La prueba de esta imprevisibilidad corresponde al deudor.

Por último las cláusulas de exoneración de responsabilidad o limitativas de derechos han de ser inequívocamente conocidas por el cliente o persona que contrate con el banco o entidad financiera y redactadas en forma tan clara y precisa que su asunción no ofrezca la menor duda.

Todas estas precisiones expuestas basadas en declaraciones jurisprudenciales, son de aplicación en relación con las cláusulas de exoneración de responsabilidad en contratos de transferencia de fondos. No es admisible en ningún momento, como se ha visto, una exclusión generalizada y sin límites de responsabilidad por parte del banco o entidad financiera en perjuicio del cliente. *Cfr. Sentencias del Tribunal Supremo de fechas: 16 de julio de 1992, 20 de julio de 1992, 11 de febrero de 1992 y 28 de abril de 1992.*

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

exoneración de responsabilidad en los contratos referentes a transferencias electrónicas de fondos debe estudiarse en coordinación con el sistema legal vigente en cada país. Pero con carácter general se puede afirmar que las cláusulas de exoneración de responsabilidad establecidas en contratos entre los bancos, entre los bancos y otras entidades que participan en el proceso de transferencia de fondos, y entre los bancos y sus proveedores de software o de hardware, no surten efectos en las relaciones entre el banco y sus clientes. El cliente debe estar facultado para presentar su reclamación a aquella entidad que causó la pérdida por sus actos u omisiones, sin tomar en consideración cláusulas de exoneración existentes en contratos en los que el cliente no es parte.

Los fraudes cometidos en una transferencia de fondos pueden venir originados por la manipulación del equipo físico informático o por la manipulación de los elementos lógicos del sistema. Pero normalmente la responsabilidad no se enfoca de esta manera, por manipulaciones, sino que se pacta que el banco quedará exonerado de responsabilidad cuando no se cumpla debidamente una orden de transferencia de fondos si puede probar que hubo un fallo del equipo físico o la dotación lógica de la computadora. Nada se dice sobre el origen de dicho fallo, si ha de ser debido a fuerza mayor o también se incluye el originado por una manipulación fraudulenta. En este segundo caso la exoneración de responsabilidad por parte del banco es inadecuada pues, como antes se ha expuesto, es el banco originario el que elige el conducto adecuado para llevar a efecto la transferencia de fondos. Incluso con el alto nivel de automatización existente hoy en casi todas las entidades financieras, la elección de esa vía puede producirse de forma automática por un ordenador de la propia entidad financiera, deberá ser esta entidad la que asuma también la responsabilidad del buen término de la operación. La entidad deberá ejercer una prudencia razonable en la selección de los medios apropiados para efectuar la transferencia, si esta prudencia falta y a consecuencia de ello se produce el fallo físico o lógico del sistema, la responsabilidad debe atribuirse a dicha entidad. Igual debe ocurrir si el fallo ha tenido su origen en una manipulación fraudulenta. Lo que sí puede fundamentar una exoneración de la responsabilidad del banco es un fallo general o un desastre de gran magnitud.

Por tanto, el banco o entidad financiera, serán responsables del correcto funcionamiento de su equipo físico y lógico en la realización de la transferencia de fondos. El mantenimiento en correcto estado de conservación de este equipo y su vigilancia para su uso exclusivo por personal autorizado, es responsabilidad del banco originario exigible tanto por vía contractual como extracontractual.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Si estas consideraciones deben hacerse en relación con las manipulaciones de software y hardware que pueden afectar a operaciones de transferencia electrónica de fondos, no resulta de menor interés la determinación de la responsabilidad del banco originario en las manipulaciones en la transmisión. En casi todas las transferencias electrónicas de fondos interbancarias y en la gran mayoría de las intrabancarias se recurre a un servicio de telecomunicación de datos. Parece que es una situación ampliamente extendida la de exoneración de responsabilidad de las empresas de telecomunicación por daños producidos por fraude en la transmisión o por cualquier otra anormalidad en el transporte de los datos. La empresa de telecomunicación se escuda, para fundamentar esta exoneración, en la imposibilidad de prever las consecuencias de la anormalidad en la entrega del mensaje, entre otras razones porque la empresa de telecomunicación desconoce el contenido del mensaje que transporta.

Asimismo constata el documento de la CNUDMI cómo en muchos países los servicios de telecomunicación han sido prestados por el Estado. De este modo el servicio de telecomunicaciones se ha beneficiado del régimen de exención de responsabilidad general del Estado. Incluso en algunos casos el régimen de exención general se reforzaba con reglamentación específica para proteger el servicio de telecomunicaciones. También se ha producido la limitación de responsabilidad en los países donde la explotación de los servicios de telecomunicaciones correspondía a empresas privadas. Pero hoy ya la situación de monopolio de las empresas de telecomunicaciones toca a su fin[96]. El mercado de

[96] Pues bien el último documento comunitario sobre la situación del sector de servicios de telecomunicación asume este objetivo y propone una meta aún más audaz: conseguir la **total liberalización del servicio público de telefonía** en el ámbito comunitario. Debemos tener en cuenta que una red telefónica puede y de hecho hoy es una red adecuada de comunicación de datos para transferencias electrónicas de fondos.

La Comunidad fija como objetivos a corto plazo los siguientes: realización de una oferta de red abierta (Open Network Provision = ONP) y el desarrollo de las comunicaciones por satélite. Como objetivo a largo plazo fundamental se recoge la liberalización de todos los servicios públicos de telefonía vocal. Pero junto a este objetivo de liberalización se enuncia el de armonización.

La oferta de red abierta queda regulada en dos Directivas fundamentales: la 90/387/CEE del Consejo de 28 de junio de 1990 relativa al establecimiento del mercado interior de los servicios de telecomunicaciones mediante la realización de la oferta de una red abierta de telecomunicaciones y la Directiva 92/44/CEE del Consejo de 5 de junio de 1992 relativa a la aplicación de la oferta de red abierta a las líneas arrendadas. Los usuarios deben tener la posibilidad de elegir entre distintos proveedores de servicios sin preocuparse de la diferencia de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

servicios de telecomunicación se liberaliza y el interrogante que se plantea es si debe seguir manteniéndose esta situación de exención de responsabilidad.

---

normas en las interfaces entre estas redes. La Directiva 90/387/CEE sobre la ONP pretende por tanto establecer una **infraestructura europea de telecomunicaciones armonizada y competitiva** lo que se puede afirmar **constituye el requisito previo para el desarrollo de los sistemas de transferencia electrónica de fondos.** Si una infraestructura armonizada de telecomunicaciones es necesaria para el posterior adecuado desarrollo de la contratación EDI y la liberalización de las telecomunicaciones es otro principio imperante en este sector, la adopción de actos por las Instituciones de la Comunidad que obliguen a los Estados miembros a armonizar sus legislaciones es absolutamente necesario. Resulta de gran interés en este tema la Directiva 90/387/CEE.

En los considerandos que preceden a la Directiva se determina la vital importancia que para la realización del mercado interior tiene el establecimiento de una auténtica libre circulación de servicios de telecomunicaciones. El establecimiento de un mercado común de servicios de telecomunicaciones implicará que cualquier restricción al derecho de prestar servicios en un Estado miembro o entre Estados miembros tiene que estar objetivamente justificada, respetar el principio de proporcionalidad y no resultar desmesurada con respecto al objetivo perseguido. Así queda en este punto recogida la auténtica esencia del concepto de red abierta de telecomunicaciones: un **derecho de libre prestación de servicios de telecomunicación** reconocible en todos los Estados miembros de la Unión Europea. Pero este derecho que se podría calificar de fundamental en el sector de las telecomunicaciones viene acompañado de una serie de **principios** que ya comienzan a perfilarse en esta Directiva, se depuran en la Directiva 92/44/CEE y se concretan con especial claridad en la Resolución del Consejo de 7 de febrero de 1994 relativa a los principios del servicio universal en el sector de las telecomunicaciones. Así mismo se configura como objetivo fundamental en la Unión el desarrollo de **servicios panaeuropeos**, de acuerdo con esto la Unión apoya y estimula el crecimiento de los servicios de telecomunicación transfronterizos.

Las condiciones de la oferta de red abierta deberán cumplir unos principios básicos : deberán basarse en criterios objetivos, deberán ser claras y ser publicadas de forma adecuada, deberán garantizar la igualdad de acceso y no deberán ser discriminatorias con arreglo al derecho comunitario. La garantía de igualdad de acceso implica la no restricción salvo por razones basadas en requisitos esenciales, es decir, razones de seguridad en el funcionamiento de la red, mantenimiento de la integridad de la red, interoperabilidad de los servicios y protección de los datos. Únicamente estas razones pueden justificar una restricción individual de acceso a una red o a un servicio público de telecomunicación. El enunciado de estos principios supone no reconocer excepciones tampoco en el régimen de responsabilidad de los prestadores de estos servicios.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

2.3.2. RECOMENDACIÓN DEL CONSEJO DE EUROPA R(89)9 SOBRE CRIMINALIDAD INFORMÁTICA.

La cuestión de la criminalidad informática fue inscrita en el programa de trabajo del Comité europeo para los problemas criminales. Este Comité a su vez creó otro comité restringido encargado de estudiar la cuestión. El Comité restringido de expertos sobre la criminalidad en relación con el ordenador comenzó sus trabajos en 1985 y los acabó en marzo de 1989. El informe presentado por este comité restringido fue aprobado por el comité europeo para los problemas criminales y posteriormente por el comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

La Recomendación número R(89)9,[97] expone una característica fundamental común a toda la delincuencia informática en general y que también afecta en particular al fraude informático: el carácter transfronterizo que tienen todas estas conductas. Ya se apuntaron al final del primer capítulo algunos problemas que planteaba para el derecho internacional la determinación del lugar de la comisión de una manipulación de datos o de programas informáticos cuando los hechos se han realizado en distintos Estados gracias a los procedimientos de comunicación a distancia. A éste hay que añadir el problema consecuente de determinar la ley aplicable a esas manipulaciones y el foro competente para conocer de dichas actuaciones fraudulentas. Si todas estas cuestiones se plantean es por el carácter transfronterizo de la delincuencia relacionada con el ordenador. Se perfila así la necesidad de una armonización más estrecha de las legislaciones de los distintos países y una mejora en la cooperación jurídica internacional. El Comité de Ministros del Consejo de Europa toma en cuenta un informe de la OCDE[98] realizado sobre la base de una encuesta hecha por cuestionario en los Estados miembros de la OCDE, donde se presentan las grandes líneas de la política legislativa de lucha contra la criminalidad informática, así como ciertos aspectos internacionales de la criminalidad ligada al ordenador. Este informe contiene

[97] Recomendación número R(89)9, del Comité de Ministros del Consejo de Europa a los Estados miembros *Sobre la Delincuencia Relacionada con el Ordenador*, adoptada por el Comité de Ministros el 13 de septiembre de 1989, durante la 428 reunión de los delegados de los Ministros.

[98] Informe de la OCDE, P II C n° 10, sobre *El Fraude unido a la Informática: análisis de políticas jurídicas*. 1986.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

también algunas sugerencias para la adopción de una política jurídica común en los Estados miembros de la OCDE. A este respecto propone una lista de actos que deben considerarse por los distintos Estados miembros como constitutivos de delitos relacionados con la informática. A continuación se recogen, únicamente, aquellos actos constitutivos de formas de fraude informático:

1°. La entrada, alteración, ocultamiento y/o la supresión de datos y/o programas informáticos, efectuado todo ello a sabiendas con la intención de realizar una transferencia ilegal de fondos o de otro objeto de valor.

2°. La entrada, alteración, ocultamiento y/o la supresión de datos y/o programas informáticos efectuados a sabiendas con la intención de cometer una falsificación.

3°. El acceso a un programa informático y/o de telecomunicaciones o la interceptación de un sistema teleinformático, hecho a sabiendas y sin la autorización del responsable del sistema.

En todas las conductas descritas en el informe de la OCDE se observa como denominador común la realización de los hechos a sabiendas ,es decir, con dolo penal y la agresión a la integridad y estado original de los datos y programas informáticos. La finalidad perseguida puede ser variada pero la agresión se lleva a cabo sobre unos mismos objetos datos o programas informáticos. Estimamos que el informe OCDE hace una aportación fundamental, considera la protegibilidad de un bien jurídico que se perfila como de nuevo cuño , el procesamiento automático de la información. De este nuevo bien que ha de considerarse protegible por el derecho trataremos más ampliamente en el punto 2.5. de este capítulo, al hablar del bien jurídico protegido en el tipo específico del fraude informático.

Siguiendo con el análisis de la Recomendación del Consejo de Europa resultan de interés los datos en ella recogidos referentes a la amplitud de la criminalidad informática y las pérdidas sufridas por esta causa. La *American Bar Association* ha realizado una encuesta sobre cerca de 300 sociedades e instancias gubernamentales en la cual 72 organismos han afirmado haber sido víctimas en el año 1988 de infracciones informáticas. La estimación de las

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

pérdidas anuales sufridas por estas infracciones oscilan entre 145 y 730 millones de dólares. Un estudio de 1981 del *Local Government Audit Commission* en Inglaterra demuestra que, sobre 320 firmas interrogadas, el 21% ha respondido haber sido víctima de un fraude informático en los cinco últimos años. La encuesta para 1984 ha dado 77 casos de fraude que teniendo en cuenta el número de los encuestados arroja un porcentaje de un 55% de afectados por conductas constitutivas de fraude informático. En la encuesta de 1987, al menos uno de cada diez de los 1.200 organismos preguntados en el sector público y privado, ha reconocido haber sufrido fraude. La pérdida media habida por cada una de estas acciones en 1987 se aproxima a las 47.000 libras y algunas de ellas han llegado a las 100.000 libras. Una estimación prudente de pérdidas anuales registradas en el Reino Unido debida a la criminalidad informática, no incluyendo los perjuicios debidos a la pérdida o a la divulgación de datos, llega a los 30.000.000 de libras. Existen otras estimaciones que revelan cifras anuales aún mucho más elevadas.

En el curso de la Conferencia Securicom de 1988, la cifra de 3.200.000 francos ha sido comunicada por las sociedades de seguros para estimar la pérdida anual resultante de los incidentes informáticos. Según los datos dados para Francia por APSAIRD (Asamblea Plenaria de Sociedades de Seguros Contra Incendios y Riesgos Diversos), 31.000 incidentes informáticos se han producido en 1987. De ellos 20.000 han sido considerados como error humano, 9.500 como accidentes y sólo 1.500 como incidentes deliberados. Esta última categoría representa sin embargo una pérdida estimada en 3.900.000 francos franceses, representando un aumento de un 18% sobre el informe de 1986.

Es evidente que hay que manejar estas cifras con cierta prudencia vistas las grandes diferencias que existen entre ellas. Muchos estudios hechos sobre la delincuencia informática han sido criticados como poco fiables o exagerados. En cualquier caso lo que se debe pensar es que estas cifras de criminalidad informática no han disminuido en estos últimos años sino que, más bien al contrario, han ido en aumento. Se pueden citar algunos otros estudios y estadísticas oficiales relacionadas con la criminalidad informática en los Estados de la Unión Europea. Uno de estos ejemplos son las estadísticas penales de la antigua República Federal de Alemania que revelan 3.067 casos de criminalidad informática en el año 1987. De estos 3.067 casos de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

criminalidad, 2.777 se han considerado como fraudes informáticos aplicándoseles el artículo 263.a del Código Penal, la mayor parte relacionados con los cajeros automáticos. Estos datos proporcionados por la policía han dado lugar en 1987 a 150 condenas. Estas estadísticas oficiales no cubren los casos de copias ilícitas de programas informáticos. En Suecia un criminólogo ha analizado todas las infracciones graves desde 1981 a 1983. Sobre 351 casos, 38 se referían a fraudes informáticos. El ministerio austriaco del interior ha registrado 30 casos hasta finales de 1985.

Junto a estos estudios otras encuestas realizadas en la antigua R.F.A. en diez años indicaban que las pérdidas debidas a manipulaciones informáticas no autorizadas rondaban entre 200.000 y 300.000 marcos. Estudios similares en Suecia y el Reino Unido permiten llegar a la conclusión de que las pérdidas provenientes de manipulaciones informáticas son por término medio más elevadas que las producidas por fraudes tradicionales.

Ahora bien, todo lo dicho hasta aquí debe de entenderse con la siguiente matización: la investigación en la cifra de la criminalidad informática se ve dificultada al no poder utilizar la vía de la consulta a los autores o a las víctimas, y siguiendo aquí a Tiedemann[99], tampoco resultan seguros los datos obtenidos de las estadísticas extrapenales. La Recomendación del Consejo de Europa continúa haciendo algunas precisiones en relación con el autor de estas conductas delictivas. Frente a las afirmaciones hechas por algunos estudiosos del tema en el sentido de que los crímenes informáticos más graves son obra de personas muy competentes, con formación universitaria, se defiende otra postura apoyada en datos estadísticos que muestra cómo a menudo el autor de la infracción es un empleado de la víctima que conoce bien los entresijos de la empresa. Se trata de una persona habituada a cambiar

[99] TIEDEMANN, Klaus. *Lecciones de Derecho Penal Económico. (Comunitario, español, alemán)*. PPU. Barcelona, 1993. Pág. 271 y ss. Como vía más adecuada de investigación de la denominada cifra negra en la criminalidad informática y en general en la delincuencia económica, este autor apunta el método iniciado por *Magnusson* en Suecia según el cual el investigador examina con el permiso de la correspondiente autoridad un número amplio de presupuestos económicos. Este es un proceso económicamente muy costoso "y sólo puede ser aceptado cuando se llega a comprender que la carga criminal en los diferentes ámbitos económicos es significativamente más grande que la estimación que se ha tenido hasta ahora". Esta reflexión dedicada a la criminalidad económica en general es adecuada también para la criminalidad informática.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

frecuentemente de empleo, no identificándose, por tanto, con la empresa donde trabaja. La motivación para cometer el fraude en sentido estricto únicamente puede ser una motivación puramente económica, si la motivación es la venganza estaríamos ante otra figura delictiva, el sabotaje informático.

Ante la situación descrita la evolución internacional en materia de criminalidad informática ha seguido distintos caminos en los Estados miembros del Consejo de Europa, como bien pone de manifiesto la Recomendación. En la mayor parte de estos Estados el fenómeno nuevo que constituye la criminalidad informática ha suscitado aproximadamente desde comienzos de la década de los ochenta un debate sobre si el derecho penal interno ofrece un arsenal jurídico suficiente para combatir los nuevos tipos de delitos, o por el contrario, si es necesaria una adaptación y desarrollo de este derecho[100].

La Recomendación del Consejo expone cómo varios Estados miembros han mejorado su derecho penal positivo, entre ellos Austria, Dinamarca, Francia, la desaparecida R.F.A., Grecia, Liechtenstein, Noruega y Suecia. Mientras otros lo han complementado con medidas aisladas entre ellos España[101]. Conviene aquí precisar un poco más estas referencias.

La **Ley austriaca** de 22 de diciembre de 1987 establece un delito de sabotaje informático definiéndolo como el perjuicio obtenido a través de alteración, cancelación, inutilización y ocultación de datos sobre los que no se tiene

[100] En este marco de necesidad de armonización de la legislación de los países europeos en materia de control legal frente a abusos provenientes del sector de la informática, se enmarca el denominado Tratado Schengen en el que se acuerda la supresión gradual de los controles en las fronteras para el intercambio de datos. Esta supresión de controles será posible si los estados reconocen niveles coincidentes de protección de los datos personales. Se pone de manifiesto aquí claramente la necesidad de uniformidad en el tratamiento legal del fenómeno informático. El protocolo de adhesión del Gobierno del Reino de España al acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985 fue ratificado por España el 25 de junio de 1991 y ha sufrido una modificación el 6 de noviembre de 1992.

[101] Tras la entrada en vigor del Nuevo Código Penal español la situación ha variado sustancialmente.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

disponibilidad. Autor del delito, sigue diciendo la ley, es aquél que no tiene el derecho de disposición total sobre los datos. Este delito queda establecido en la ley como un delito de resultado y las penas a imponer se harán en cuantía proporcional al perjuicio causado. De este modo la Ley de 22 de diciembre de 1987 bautiza con el nombre de sabotaje informático una serie de conductas que en sus características coincide con las manipulaciones de registros informáticos, elemento fundamental del fraude informático.

Otro país de nuestro entorno socio-cultural como es **Francia** recoge en una ley de 5 de enero de 1988[102] la figura delictiva del sabotaje informático entendiendo éste como el impedimento o falsificación del funcionamiento de un sistema de tratamiento de datos con el ánimo de causar lesiones, o la introducción, supresión o alteración de datos en un sistema de tratamiento automatizado. Esta ley a diferencia de la austriaca deja más claro cuál ha de ser el móvil para la acción, en el caso del sabotaje el ánimo de lesión a tercero. Aquí radica una de las diferencias fundamentales entre sabotaje y

[102] La ley nº 88-19 de 5 de enero de 1988 relativa al fraude informático tipifica nuevos delitos pertenecientes al ámbito de la delincuencia informática. La ley de 5 de enero de 1988 tiene una vocación de universalidad abarcando en su contenido no únicamente la figura del fraude informático, sino otras como el sabotaje, ataques a las libertades individuales, violación de secretos, etc. Esta ley ha contribuido a reforzar en Francia la necesidad de desarrollo de un derecho penal específico de la informática. Con esta ley se creó el Capítulo III del Título II del Libro III del Código Penal francés con el título: "ciertas infracciones en materia de informática". Estas infracciones no han sido individualizadas con extrema precisión pero sí se pueden distinguir seis conductas que vienen sancionadas por la ley: acceso fraudulento a un sistema informático (art. 462-2); acceso fraudulento a un sistema provocando la alteración de los datos en él contenidos (art. 462-2); alteración voluntaria del funcionamiento de un sistema informático (art. 462-3); alteración voluntaria de los datos de un sistema (art. 462-4); falsificación de documentos informáticos (art. 462-5); uso de documentos informáticos falsificados (art. 462-6). Toda esta amplia casuística puede verse reducida a las siguientes dos categorías de conductas delictivas: acceso a un sistema informático con el fin de conocer la información en él almacenada y acceso a un sistema informático con el fin de modificar la información almacenada en dicho sistema. La manipulación de un sistema informático, que sería la conducta más cercana a lo que nosotros hemos definido como fraude informático, queda definido su contenido en la ley francesa en tres ámbitos: la perturbación del tratamiento de datos, la alteración de los datos y la falsificación de los resultados. Por último, en relación al sistema de penas previsto por esta ley se penaliza la tentativa del delito informático. Así mismo se establece como pena accesoria la confiscación de los materiales que hayan servido para la comisión de la infracción.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

fraude, en el ánimo del autor. En el fraude el ánimo que mueve al ejecutor es el lucro y en el sabotaje es el ánimo de lesionar los intereses patrimoniales de un tercero.

Por último, también en **Alemania,** se define el sabotaje informático pudiendo ser cometido éste por la alteración, inutilización, cancelación y ocultación de los datos; o a través de la destrucción o el deterioro del sistema de elaboración de los datos. Parece, a la vista de estas breves referencias, que el sabotaje informático cuenta en comparación con el fraude informático con una más depurada regulación en el derecho comparado.

Fuera del Consejo de Europa son destacables las leyes adoptadas en Australia, Canadá, y Japón, así como numerosas mejoras aportadas por el derecho federal de USA y por el derecho de cada uno de sus Estados.

El análisis de los derechos penales nacionales por un grupo de trabajo de la OCDE, señala zonas de convergencia sobre las cuales es posible elaborar unas recomendaciones a nivel internacional. Esto lleva a elaborar unas estrategias comunes en la lucha contra esta criminalidad:

1º. Es necesaria la definición o tipificación de los actos constitutivos de nuevos delitos o bien la mejora y complemento del derecho penal positivo.

2º. Establecimiento de un sistema eficaz de persecución de estas conductas siendo necesaria una revisión de los procedimientos penales internos.

3º. Estrechamiento de la colaboración internacional en la lucha contra este tipo de criminalidad.

En la lucha contra la criminalidad europea en general, y particularmente la criminalidad informática, es obligado mencionar el Tratado Schengen relativo a la supresión gradual de los controles en las fronteras comunes[103].

[103] Protocolo de adhesión del Gobierno del Reino de España al Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985, tal como quedó enmendado por el Protocolo

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Una vez recogida la parca reglamentación sobre este fenómeno del fraude informático y la escasa, aunque muy esclarecedora, jurisprudencia nacional aparecida, el desarrollo de este punto girará fundamentalmente alrededor del estudio que la doctrina ha hecho de este fenómeno. Entendiendo la expresión "fenómeno" en el sentido de análisis de la casuística y deducción de las características y elementos del fraude informático de esta misma casuística.

2.4. EL BIEN JURÍDICO PROTEGIDO EN EL TIPO ESPECIFICO DEL FRAUDE INFORMATICO

Aunque ya se cuenta en Derecho español con un artículo, el 248.2, en el Nuevo Código Penal que en opinión de autorizada doctrina, Prof. Bueno Arús[104], configura como delito de estafa tradicional el fraude informático, todavía dada la reciente entrada en vigor del mencionado precepto no existe jurisprudencia que aplique, interprete y aclare el mismo. En cualquier caso lo que sí es claro es que el legislador ha optado por tipificar las conductas de fraude informático utilizando un delito tradicional como es la estafa. Pese a ello defendemos que en relación con las conductas delictivas del fraude informático, es fundamental distinguir en éstas un bien jurídico protegido independiente, para de este modo poder reivindicar la autonomía de la figura del fraude informático de otros delitos patrimoniales como por ejemplo la estafa.

Sostenemos que el bien jurídico protegido es el procesamiento automático de la información. La información y su procesamiento automático, hoy se configuran como bienes de carácter patrimonial. La integridad y confidencialidad de la información son bienes jurídicamente protegibles con importantes repercusiones patrimoniales. El bien jurídicamente protegido no solo es la información en su estado de "reposo", sino también, los tratamientos a que es sometida por los sistemas automatizados de carácter informático. Por tanto nos referimos a la protección o a la protegibilidad de la información en su doble aspecto estático,

---

de Adhesión del Gobierno de la República Italiana firmado en París el 27 de noviembre de 1990, hecho en Bonn el 25 de junio de 1991. BOE 30/07/1991 N° 19399.

[104] *Actualidad Informática Aranzadi*, n° 11.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

integridad y confidencialidad, y en su aspecto dinámico, proceso y transmisión de esa información[105].

No debemos olvidar la agresión a otros bienes jurídicos tradicionales como son el patrimonio y la fe pública necesaria en el tráfico jurídico[106].

2.5. ELEMENTOS BÁSICOS DEL TIPO. (Características, elementos identificadores)

Para el desarrollo de este punto partiremos de una referencia a la doctrina americana más reciente en este tema del fraude informático, para a continuación pasar a analizar las opiniones de los autores españoles sobre la materia.

Para DeMaio[107] el problema fundamental al enfrentarse con el estudio del fraude informático es descubrir lo específico de este fraude que lo distingue de otras modalidades de fraude.

En lo fundamental, nada distingue un fraude cometido por cualquier otro medio que no sea el medio informático. Y sin embargo es curioso comprobar cómo la mayoría de los fraudes informáticos surgen porque un individuo descubre un fallo

[105] Hablar del bien jurídico independiente del procesamiento automático de la información requiere precisar los límites de ese procesamiento. Con ánimo generalizador se puede afirmar que la filosofía de funcionamiento de los ordenadores digitales actuales ,como automatismos secuenciales de programa exterior, se resume en los siguientes cinco puntos: 1. la máquina solo sabe hacer un reducido número de operaciones elementales (de comparación de estados en la mayoría de los casos). 2. La máquina es programable, hace lo que le indique el programa en ejecución. 3. La secuencia de operaciones a realizar por la máquina viene determinada por la secuencia de instrucciones que aparezca en el programa. 4. Al ser la máquina de propósito general si se cambia la secuencia de instrucciones del programa se cambia el proceso a realizar. 5. El funcionamiento correcto de la máquina exige preservar la integridad en el funcionamiento de los elementos físicos y lógicos. De acuerdo con esta filosofía de funcionamiento el bien jurídicamente merecedor de una protección se extiende desde el momento en que las instrucciones del programa comienzan a ser ejecutadas por los elementos físicos de la máquina hasta la obtención de un resultado que es depositado en memoria.

[106] Cfr. ROMEO CASABONA, Carlos María. Op. Cit. Pág. 108 y ss.

[107] DEMAIO, Harry B. Op. cit. Pág. 191 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

o una debilidad en los sistemas de control y finalmente sucumbe a la tentación de aprovecharse de ese fallo o debilidad del sistema informático. Decimos resulta curioso en el sentido de que el origen de una acción con consecuencias o efectos económicos de magnitudes considerables provenga, en muchas ocasiones, de pequeños fallos del sistema que podrían controlarse o prevenirse con facilidad evitando así consecuencias negativas de gran envergadura.

También es verdad que han existido fraudes informáticos meticulosamente planeados por maestras mentes criminales.

Aunque en mayor profundidad trataremos el tema en el punto correspondiente a los elementos personales del fraude informático, haremos ahora algunas consideraciones sobre los autores de estos crímenes informáticos que servirán para acercarse al concepto del fraude informático. Donde quiera que el tema del fraude informático surge o aparece el primer grupo de sospechosos lo conforman los programadores de sistemas. A nadie se le escapa que son ellos los que pueden cambiar los programas que guían el sistema informático y hacer que éste sirva a sus propios fines particulares. Pero también deben tener la posibilidad de dirigir los resultados de sus acciones ilícitas para su propio provecho. Esto, por lo general, implica algún tipo de acceso y ,manipulación del sistema. La cuestión a la que se quiere llegar es que si el programador ha desarrollado o diseñado un proceso informático fraudulento dentro de una aplicación pero no tiene ocasión de usarlo, no obtiene ningún beneficio de todo ello. Con esta argumentación DeMaio llega a la conclusión de que la mayoría de los fraudes informáticos se llevan a cabo por usuarios y otras personas con acceso a las aplicaciones. La cuestión es que los programadores no son omnipotentes en el sentido de control absoluto, total, de todo el sistema informático. Normalmente tendrán una parcela de funciones asignada bien definida y el introducir un proceso fraudulento implica, o hace necesario, tener acceso a todas las fases de desarrollo del proceso.

Hay distintos tipos de fraude. El más simple supone cambiar un valor en un registro: montante de un crédito, registros sobre empleo, datos de la Seguridad Social... El defraudador simplemente cambia el dato y el sistema informático se encarga de hacer el resto. Se está refiriendo aquí el autor a manipulaciones de los datos de entrada, manteniéndose el proceso y el sistema de obtención de resultados invariable. Ahora bien teniendo en cuenta que si lo que entra y procesa el sistema es "basura" el resultado será también "basura".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Hay otras muchas formas de fraude, tales como generar documentos de pago para compañías inexistentes. Esto supone crear una completa serie de documentos base en que se apoyen esos documentos de pago o con valor solutorio, es decir, dar una apariencia de realidad a todo el conjunto.

Los controles establecidos en el sistema informático deben ser manejados con cuidado de forma que no comprueben todo el proceso desde la fuente o el origen. Los controles no deben poder retroceder hasta el origen del proceso.

Una de las formas de fraude más mencionadas y usadas es la técnica "salami". Es una forma de fraude que altera pequeñas cantidades en procesos habituales y correctos como abono de intereses en cuentas corrientes, etc. La técnica salami consiste fundamentalmente en vez de redondear hacia arriba una cantidad, los autores de estas acciones paran el proceso, detraen el resultado del redondeo de la cifra y lo trasladan a una cuenta especial que se ha creado previamente al efecto. Céntimo a céntimo sobre un espectro de varios cientos de miles de cuentas supone grandes sumas.

Para llevar a cabo cualquiera de estas manipulaciones los sistemas de control han de ser burlados. Evidentemente el autor de estas defraudaciones debe conocer qué pueden detectar los sistemas de control y qué no pueden detectar. Se han de desentrañar las bases de autorización, control de acceso, separación de funciones,...

Un punto débil, de algunos sistemas a tener muy en cuenta son los denominados "default options", las opciones por defecto. Estas opciones abren procesos en principio prohibidos o inexistentes, pero que en la práctica permiten desarrollar de forma paralela a las opciones controladas, otras sin dicho control. Por ejemplo en una pantalla de menú general con ocho opciones lo normal será que el usuario elija una de ellas de entre la uno a la ocho pero ¿qué ocurre si el usuario pulsa la tecla nueve de una supuesta opción que realmente no existe? Si el proceso está bien diseñado debería ofrecer un mensaje de error y reconducir a la misma pantalla de opciones generales de la uno a la ocho en el ejemplo que vengo siguiendo.

Pero esto a veces no ocurre así y al pulsar una tecla de una opción inexistente, el sistema permite al usuario crear su propia operación sin seguir ninguna de las

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

opciones previstas. Esto es lo que se denominan "open-ended options" o lo que es igual, opciones inacabadas abiertas que permiten un reconocimiento como usuario legítimo del sistema a un tercero, que sin seguir ninguna de las opciones previstas y, por tanto, sin salvar ningún control entra en el sistema y realiza libremente las operaciones o transacciones que éste permite.

Para evitar este tipo de situaciones, que más que una auténtica manipulación (de datos o de programas) se trata de aprovechar un defecto en el diseño del sistema de acceso, DeMaio propone cerrar todas las puertas de acceso al sistema. Es decir las opciones de menús que se presentan al usuario. Todos los menús deben encontrarse en estado "closed-ended". Es decir dotar de rigidez al sistema de acceso.

Este autor hace referencia a la técnica "salami" como manipulación tanto de datos como de programas que tratan esos datos (redondeo de cifras), manipulaciones de datos en general y por último el aprovechamiento de resquicios del sistema para el desarrollo de procesos incontrolados.

Otro conjunto de situaciones que deben atenderse con especial cuidado son aquéllas en las que se presenta una parte de un programa para su posterior desarrollo y sólo se verifican las funciones fundamentales de dicho software y se olvidan aquellas otras funciones que por su nivel más avanzado, o por su poca aparente utilidad se prevé tendrán escasa utilización en la práctica.

Permitir a los programadores diseñar sus propios tests sin una supervisión o sin ajustarse a unos standars es una invitación hecha para el debilitamiento de los controles. El programador puede no ser deshonesto, pero lo cierto es que existen en toda aplicación anomalías ocultas que están esperando que alguien las descubra.

DeMaio continúa con este repaso de posibles vías de comisión de fraudes informáticos preguntándose cómo puede ocurrir que aparezcan fallos en programas después de dos o tres años de desarrollo de los mismos. Probablemente la razón se encuentra en que es la primera vez que un especial conjunto de circunstancias se han producido simultáneamente provocando la aparición del fallo. Otra situación puede ser aquélla en la que el fallo se creó como resultado de cambios introducidos en el sistema. Esta es la razón por la que los **controles periódicos** son tan

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

importantes. Controles que deben extenderse no sólo a las innovaciones sino también a todo el conjunto de funciones para, de este modo, asegurarse que el nuevo código no afecta a otra función.

No trataremos en este capítulo del fraude informático de la actuación de los denominados "hackers". Individuos, que en muchas ocasiones, tienen un profundo sentido anti-institucionalista. Para muchos su función en la vida es derribar las instituciones (entiéndase grandes empresas, Gobierno, compañías telefónicas). El ánimo de lucro en raras ocasiones aparece y, por tanto, aparta a esta categoría de criminales y a sus actuaciones de nuestro ámbito de interés. También hay "hackers" que simplemente actúan por curiosidad o irresponsabilidad. Sigue, por tanto, excluyéndose como motivación fundamental el ánimo de lucro.

De lo expuesto se deducen las **características** fundamentales del **fraude informático** que coincidiendo con la exposición del Prof. Bueno Arús[108] se pueden sintetizar en las tres siguientes:

1ª. Manipulación de datos informáticos.
2ª. Animo de lucro.
3ª. Perjuicio patrimonial para tercero.

Si alguna de estas tres características no se cumple, en la acción que se esté analizando, no se podrá calificar dicha acción como fraude informático.

Utilizando una terminología similar aunque no idéntica Domínguez[109] resume las siguientes características del fraude informático: es un acto intencionado consistente en la manipulación y alteración de registros informáticos realizado dicho acto con ánimo de lucro. Precisa un poco más este autor en relación con el elemento de la manipulación de los datos o "Data Didding" diciendo que ésta puede ser llevada a cabo de dos formas: o bien alterando los datos de entrada al

---

[108] BUENO ARUS, Francisco. *El Delito Informático*. Revista Actualidad Informática Aranzadi. Nº 11, abril 1994. Madrid. Páginas 1 y ss.

[109] DOMINGUEZ, Agustín. *Transferencia Electrónica de Fondos y de Datos. Protección jurídica de los datos personales emitidos en una operación de pago electrónico*. En vol. Encuentros sobre Informática y Derecho 1992-1993. Coor. M.A. DAVARA. Aranzadi. Pamplona. 1993. Página 119 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ordenador o bien alterando los datos durante el proceso. También reconoce este mismo autor que dentro del sistema de comunicación puede existir una manipulación de los datos de tal forma que la información que llega al ordenador destino no coincide con la información que salió del ordenador emisor.

2.5.1. ÁNIMO DE LUCRO

En el fraude informático, como en los delitos económicos en general, cobra una trascendental importancia el ánimo de lucro o *animus defraudandi* como elemento subjetivo del injusto de carácter esencial. El ánimo de lucro consiste sustancialmente en la intención de obtener, para sí o para otros, un enriquecimiento, beneficio o ventaja de índole patrimonial o económica[110].
El ánimo de lucro es, por tanto, un elemento subjetivo que ha de encontrarse presente en el agente de la conducta ilícita. Se denomina indistintamente ánimo de lucro, apropiación o defraudación, o también *animus rem sibi habendi*, que se resume en la conciencia y voluntad de disponer de la cosa como propia[111].

El ánimo de lucro no se presume siempre en todo indebido o no justificado apoderamiento de una cosa ajena, pero si no se demuestra que era otro el propósito del agente, es racional entender que en su comportamiento de apropiación de bienes de pertenencia de otra persona medió ánimo de lucro[112].

Debe asimismo tenerse en cuenta que el ánimo de lucro, al que venimos haciendo referencia, puede consistir en cualquier ventaja, utilidad o beneficio, incluso de finalidad meramente contemplativa o de ulterior beneficencia o liberalidad.

En la jurisprudencia del Tribunal Supremo el concepto de ánimo de lucro no puede ser de mayor amplitud y elasticidad, haciéndole sinónimo de cualquier

---

[110] Cfr. Sentencia del Tribunal Supremo de 16 de marzo de 1989. Sala segunda.

[111] Cfr. Sentencia de la Sala 2ª del Tribunal Supremo de 30 de Mayo de 1990. Ponente: Sr. Sierra Gil de la Cuesta.

[112] Cfr. Sentencia de la Sala 2ª del Tribunal Supremo de 20 de marzo de 1990. Ponente: Sr. Cotta y Márquez de Prado.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

provecho, beneficio, ventaja o utilidad, incluso, como ya hemos visto, altruista o comtemplativa. Es, así mismo, indiferente que se actúe con finalidad de obtención de beneficio para sí mismo o para tercero[113].

De acuerdo con lo dicho todas las conductas que se califiquen de fraude informático deberán estar presididas por el ánimo de lucro como elemento esencial del injusto.

Este ánimo de lucro es requisito común a todos los delitos patrimoniales que pueden agruparse bajo la denominación de delitos de enriquecimiento. Estos delitos de enriquecimiento de suyo implican el consiguiente perjuicio patrimonial para un tercero.

En conclusión el ánimo de lucro se presenta como el elemento subjetivo del injusto y en la característica determinante del dolo específico que implica el deseo y la intención de obtener un beneficio patrimonial o una ganancia evaluable económicamente.

2.5.2. ENGAÑO

El elemento del engaño ha sido tratado por la jurisprudencia en relación con el tipo de la estafa. El engaño en la estafa, precedente o concurrente, constitutivo de la *ratio esendi*, es el núcleo y alma del tipo.

En la estafa, el engaño se ordena a crear una apariencia de realidad, sin embargo en las conductas de fraude informático no hay que aparentar una realidad sino falsearla. El engaño por tanto se traduciría en el falseamiento de unos datos o de un proceso real que se lleva a cabo electrónicamente.

No se debe olvidar que el engaño que nació con la finalidad de obtener un beneficio va unido a la producción de un perjuicio[114]. Perjuicio que ha de

[113] Cfr. Sentencias de la Sala 2ª del Tribunal Supremo de fechas: 31 de diciembre de 1974, 3 de octubre de 1978, 30 de mayo de 1980, 10 de marzo de 1981, 20 de junio de 1985, 10 de junio y 19 de octubre de 1987 y 25 de enero de 1988.

[114] Cfr. Sentencia de la Sala 2ª del Tribunal Supremo de 1 de febrero

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

entenderse como una disminución patrimonial clara si se compara la situación del perjudicado antes y después de la consumación del fraude. Con esto conectamos dos de los elementos del fraude: el engaño y el perjuicio para tercero.

2.5.3. DOLO. INTENCIÓN DE MANIPULAR REGISTROS INFORMATICOS.

La acción dolosa lleva consigo dos elementos fundamentales: uno de carácter intelectual, intencional, es decir, saber lo que se está haciendo y un segundo elemento volitivo o emocional, querer realizar la acción.

La cuestión que debe estudiarse en las conductas calificables de fraude informático es la determinación de los elementos que deben verse abarcados por el dolo.

Para la jurisprudencia del Tribunal Supremo el dolo en los denominados delitos de enriquecimiento debe estar referido a la ajenidad de la cosa y al propósito de incorporación de ésta al propio patrimonio[115]. En el fraude informático el dolo por tanto debe abarcar el conocimiento de que se está tratando con una cosa ajena.

2.5.4. POSIBILIDAD DE PERJUICIO PATRIMONIAL PARA LA VICTIMA

El fraude informático exige como requisito *sine qua non* la existencia en la dinámica originadora del ilícito de dos personas contrapuestas, el sujeto activo y el pasivo. El primero productor de un engaño y el segundo perjudicado por ese engaño.

El acto de fraude informático, como acto deliberado de manipulación de

---

de 1993. Ponente: Sr. De Vega Ruíz.

[115] Cfr. Sentencia de la Sala 2ª del Tribunal Supremo de 12 de noviembre de 1990.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

registros o de una falsa representación de una realidad, con ánimo de engaño y con intención de lucro, se realiza siempre en detrimento de una persona física o jurídica. Y la víctima sufre una pérdida económica que afecta directamente o indirectamente a su patrimonio. Si en una conducta no podemos apreciar estas características no podemos calificarla como fraude informático.

2.5.5. INFORMÁTICA COMO MEDIO PARA LA COMISIÓN DEL FRAUDE.

El ordenador o el entorno informático deben encontrarse siempre involucrados de una manera directa o indirecta en la comisión del fraude.

Es la comisión del fraude a través del medio informático lo que especifica esta figura convirtiéndola en independiente de otras. Es por tanto la utilización del medio informático lo que eleva a una categoría independiente este tipo de ilícitos. Esto es así ya que la informática proporciona a la acción una serie de características del todo nuevas. Por ejemplo las posibilidades de ocultación de la acción injusta se aumentan con el uso de la informática, el delito se produce incruentamente con la obtención de altos beneficios, el delincuente se ve amparado por sus propios conocimientos técnicos que le dan una sensación de impunidad, además debemos recordar que la mayoría de los fraudes informáticos no son denunciados[116], lo cual constituye un estímulo para los

[116] Esta situación ha variado tras la generalización en el uso de la red mundial Internet. La utilización de esta red ha traído indudables ventajas culturales y comerciales a sus usuarios pero también es un campo "virgen", sin regulación, donde sin duda se han cometido, se cometen y cometerán delitos. Sin embargo estas conductas no se ocultan sino que se debaten. Así existen desde noviembre de 1988 los denominados CERT (Computer Emergency response Team) o IRT (Incident Response Team) que fueron creados por la Agencia de Investigación en Proyectos Avanzados (ARPA) en respuesta a las necesidades planteadas ante un incidente de seguridad en Internet. Ante una incidencia en Internet es necesario un equipo de respuesta inmediata que minimice los efectos del ataque, recuperando, si es posible, la información perdida y determinando la información que se ha divulgado. Un IRT es un equipo que gestiona directamente un incidente producido en una determinada organización. El CERT es un centro de coordinación de incidentes de mayor envergadura, en los que se encuentran implicados varios sistemas de una o más organizaciones. La seguridad en Internet se basa en la robustez fruto de este diálogo y discusión de incidentes o ataques a la información y a los

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

defraudadores.

2.6. ELEMENTOS PERSONALES CAUSALES: SUJETO AGENTE

No es fácil encontrar un perfil único del delincuente informático, o del defraudador informático. Sin embargo se puede afirmar, a la luz de los casos reales conocidos, que debe de tratarse de una persona con unos conocimientos mínimos en la gestión de un sistema informático. Decimos conocimientos en la gestión de un sistema informático porque no es necesario conocer el funcionamiento interno del sistema pero sí su gestión externa. El defraudador puede pertenecer al personal al servicio de la empresa o bien tratarse de una persona ajena que actúa en solitario o en colusión con empleados de la entidad defraudada. En este último caso podemos estar hablando de delincuentes comunes, de organizaciones criminales o simplemente de oportunistas que han visto una manera fácil y rápida de obtener elevadas sumas de dinero. Siguiendo aquí a la doctrina más autorizada en el tema se puede afirmar que los autores de los fraudes informáticos suelen ser primarios u ocasionales[117]. De aquellos fraudes informáticos que han proporcionado mayores beneficios han sido autores, empleados de las propias empresas afectadas, que no siempre poseían conocimientos especializados en el campo del tratamiento automatizado de los datos[118]. De todas formas este dato apuntado en último lugar no debe tomarse con absoluto rigor ya que, como hemos dicho anteriormente, los expertos en informática precisamente por esa condición son capaces de encubrir con mayor facilidad su acción delictiva.

---

sistemas, y no en la ocultación como es habitual en entornos cerrados. De hecho el CERT tiene publicado su Informe Anual 1995 en el que recogen datos estadísticos sobre el número de incidentes en la Red. En concreto se señala que el CERT intervino en más de 2.400 incidentes de seguridad durante el período de enero a diciembre de 1995, en los que se vieron implicadas más de 12.000 organizaciones. Un resumen de este Informe Anual CERT 95 se encuentra accesible en Internet en la siguiente dirección: http://www.cert.org/cert.report.95.htm
Cf. MEDINA, M.; BUCH, J. *Respuesta a Incidentes de Seguridad*. Revista SIC, nº 22, noviembre 1996. Págs. 46 y ss.

[117] EISENBERG, Ulrich. *Kriminologie*. 2ª ed., Köln, 1985, pág. 788.

[118] SIEBER, Ulrich. *The International Handbook on Computer Crime*. Chischester, 1986. Pág. 11 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Pero los elementos causales de carácter personal no sólo han de entenderse referidos al agente del fraude sino también a los directivos de las empresas afectadas. No es infrecuente encontrar directivos de empresa desconocedores de la realidad de su tiempo, despreocupados frente al riesgo de la informática. Esta situación, aunque de una forma inconsciente, estimula a los defraudadores potenciales. Esta falta de visión de la realidad de riesgo que existe en una empresa en relación con la informática se constata en la falta de sistemas de control o en la existencia de sistemas de control inoperantes, en la falta de políticas y de normas específicas que determinen las atribuciones y responsabilidades de cada miembro de la estructura empresarial, un ambiente de permisividad que no sanciona con rigor al infractor.

La actitud de las víctimas de estos delitos suele ser la de un "sufrimiento callado" de las consecuencias del ilícito, es decir, de no denuncia de los pocos casos que llegan a ser conocidos[119]. Para entidades financieras, bien sean bancos o aseguradoras, incluso para el sector público (Seguridad Social) no es "rentable" airear los fraudes de que han sido víctimas. Con esta actitud en realidad lo que se está favoreciendo es la posición del delincuente y se priva al resto de los posibles futuros afectados de una información muy útil para la prevención de nuevos fraudes[120].

Vemos, por tanto, que son múltiples los factores que de forma directa o indirecta favorecen la aparición del fraude.

Aunque el epígrafe se refiera únicamente a los elementos o factores de carácter humano que pueden desencadenar la aparición de estas conductas delictivas no nos resistimos a no recoger, con una visión más amplia, otras circunstancias que pueden facilitar estas conductas. En concreto nos referimos a tres grupos de

[119] Confrontar con nota 116. En España hay dos servicios de coordinación de emergencias para organizaciones conectadas a Internet se denominan esCERT e IRIS-CERT. El esCERT da servicio a organizaciones públicas y privadas conectadas a Internet a través de proveedores comerciales. El IRIS-CERT da servicio a organismos de investigación conectados a través de la RedIRIS. Dada la existencia de diferentes CERTs, cada uno con un ámbito de actuación normalmente nacional, en 1990 se constituyó FIRST (Forum of Incident Response Team and Security Teams) para la coordinación de los diferentes CERTs.

[120] CHAMOUX, F.; CHAMOUX, J.P. *Adaptation du Droit à la vulnerabilité de l'Informatique en Europe*, "Droit et Informatique", 1984. Pág. 7 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

aspectos. Primero: el desarrollo de la informática a nivel corporativo en la empresa, es decir, la existencia de un alto grado de informatización en casi todas las empresas con la existencia de una serie de complejas aplicaciones informáticas que en ocasiones generan flujos amplios de información de difícil control. Segundo: se introduce otro nuevo factor de inseguridad con el uso creciente de las comunicaciones. Hoy en día la mayor parte de las transacciones financieras se llevan a cabo a través de sistemas de teleproceso . A este panorama que presentan los factores técnicos externos se añade la creciente descentralización y desmembramiento de la informática tradicional que viene ya produciéndose desde principios de los años 80 y que ahora conoce su momento más álgido con la extensión de la informática no sólo al ámbito profesional sino también al doméstico. Esta circunstancia sin dejar de ser un progreso evidente para el conjunto de la sociedad supone un claro peligro. Como acertadamente pone de manifiesto Sneyers[121] ha aumentado la despreocupación en el manejo del ordenador. En definitiva se está desconociendo el potencial peligro que encierra el uso abusivo[122] de los sistemas informáticos. A esta despreocupación en el uso del sistema informático hay que añadir una creencia totalmente errónea según la cual todo trabajo debe tener sus ventajas ocultas. De acuerdo con esto la empresa no debería perseguir aquellas conductas de escaso valor defraudatorio de sus empleados. Todo ello conduce a una horadación de la moral dentro del grupo de trabajo que favorece el fraude . El tercer y último factor vendría constituido por la nube que siempre oculta todos los datos relacionados con estos hechos. Se carece de datos y estadísticas fiables y actualizadas, como ya hemos puesto de manifiesto, sobre estas conductas. Pero lo peor no es no contar con estos datos sino que en muchas ocasiones estos datos no existen porque los hechos delictivos no se persiguen. El desprestigio que supondría el esclarecimiento total de los hechos pondría de manifiesto la vulnerabilidad y debilidad de las instituciones afectadas y se entiende que este daño es muy superior al resarcimiento que se lograría con el castigo del culpable. En definitiva este tercer factor de la falta de información abona el terreno para el fraude.

---

[121] SNEYERS, Alfredo. *El Fraude y otros Delitos Informáticos*. T.G.P.-Tecnologías de Gerencia y Producción. Madrid. 1990. Página 5 y ss.

[122] "Por abuso informático se entiende el uso malintencionado del ordenador por razones de lucro o de venganza y la despreocupación. El simple descuido, el error al que no se da importancia, la intromisión en los sistemas informáticos, pueden tener consecuencias muy difíciles de evaluar". SNEYERS, Alfredo. Op. Cit. Loc. Cit.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

El potencial autor de un fraude informático ve en el progreso de la informática, en los factores técnicos de su desarrollo y en la falta de información sobre hechos delictivos anteriores, el caldo de cultivo adecuado para llevar a cabo su plan criminal.

2.7. ELEMENTOS VULNERABLES: OBJETO DE LA AGRESIÓN

Como ya explicaremos con más extensión en el punto tercero al hablar de las formas típicas de fraudes informáticos 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 y la modificación no autorizada de los datos.

De acuerdo con la legislación española contra estas tres 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[123] recoge una exhaustiva reglamentación sobre el deber de secreto que ampara a los datos personales sometidos a tratamientos automatizados. Del mismo modo reconoce, en su artículo 17.1 [124], 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 20 de Junio de 1994.[125] Resulta, así mismo, muy rigurosa la sanción que prevé el artículo 16[126] del Real Decreto 1332/1994 para los datos que hayan sido recogidos o

[123] BOE 31 octubre 1992 (num. 262).

[124] "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 reclamación por los afectados ante la Agencia de Protección de Datos en la forma que reglamentariamente se determine".

[125] Real Decreto 20 junio 1994, num. 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 junio 1994 (num. 147).

[126] "Artículo 16. Bloqueo de los 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".

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

registrados por medios fraudulentos. Como *ultima ratio* el Nuevo Código Penal español recoge la **protección de la intimidad frente a los ataques de la informática** en el **artículo 197**[127].

El vigente artículo 197 tipifica como acciones básicas:

1º El apoderamiento de papeles o cartas, mensajes de correo electrónico, la interceptación de la correspondencia o la utilización de artificios, con el fin de descubrir los secretos y vulnerar la intimidad de otro.

---

[127] *"197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, MENSAJES DE CORREO ELECTRÓNICO o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las* ***penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.***

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, DATOS RESERVADOS DE CARÁCTER PERSONAL O FAMILIAR DE OTRO QUE SE HALLEN REGISTRADOS EN FICHEROS O SOPORTES INFORMÁTICOS, ELECTRÓNICOS O TELEMÁTICOS, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la ***pena de prisión de dos a cinco años*** *si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

Será castigado con las ***penas de prisión de uno a tres años y multa de doce a veinticuatro meses****, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.*

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá ***la pena de prisión de tres a cinco años****, y si se difunden, ceden o revelan los datos reservados, se impondrá* ***la pena en su mitad superior.***

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En este tipo básico, la protección de datos concernientes a la intimidad de los individuos en soporte electrónico está clara y plenamente incluido como objeto de protección. Expresamente el Código habla de "mensajes de correo electrónico" y de interceptar las telecomunicaciones. Es evidente que el medio (informático o electrónico), no puede convertirse en un obstáculo para la protección de la intimidad del individuo. La protección penal que el Código otorga en este tipo básico ha de entenderse abarca a las personas físicas y jurídicas.

2º Apoderarse, utilizar o modificar datos reservados de carácter personal que se encuentren en ficheros o soportes informáticos, electrónicos o telemáticos. El apartado 2 del artículo 197, que venimos analizando, no destaca, ciertamente, por su claridad ya que junto a las conductas señaladas penaliza el acceso, alteración y utilización en perjuicio del titular de los datos o de un tercero de éstos, que se encuentren almacenados en ficheros o soportes informáticos. Decimos que no destaca por su claridad ya que primero penaliza el apoderamiento, utilización y modificación de datos en perjuicio de tercero, sin mencionar el perjuicio al propio titular de los datos, y después recoge una conducta similar de alteración y utilización ahora ya sí incluyendo en perjuicio del titular o de un tercero.

Por otra parte, resulta también complicado el juego de las agravaciones. Estas se pueden clasificar en los siguientes grupos:

- por razón de las personas que llevan a cabo la conducta delictiva: personas encargadas o responsables de los ficheros, archivos o registros; si el sujeto agente es autoridad o funcionario público (art. 198).

- Por el carácter de los datos objeto de la agresión si revelan la ideología, religión, creencias, salud, origen racial o vida sexual.

- Por la condición del titular de los datos: menor o incapaz.

- Por el ánimo de lucro del agente.

Vemos cómo 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.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 informáticos. 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, num. 16/1993. Ambas leyes someten a la autorización del autor del programa cualquier reproducción, transformación o distribución del mismo. No son menos importantes las medidas que se 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 cómo la legislación española reconoce la antijuridicidad de las acciones de manipulación de datos y programas y sanciona estas conductas.

2.8. ELEMENTOS DE RESULTADO: EFECTOS

Las consecuencias negativas que trae consigo una acción de fraude informático no sólo se dejan ver en el terreno económico sino también, y fundamentalmente, en el terreno de la imagen pública del afectado. En este sentido Hevia y Lafuente[128] recogen un conjunto de consecuencias perniciosas para la víctima del fraude que aquí juzgamos interesante reproducir. En primer lugar la agresión a la imagen de la víctima, pero no se deben olvidar los perjuicios o pérdidas patrimoniales que puede ocasionar el fraude.

[128] HEVIA, E. LAFUENTE, J.J. *Cómo luchar contra el fraude en la empresa*. Instituto de Auditores Internos de España. Madrid. 1992. Página 20 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Un sistema informático está expuesto a sufrir toda clase de daños. Cuando se utiliza la expresión "daños" no sólo nos estamos refiriendo a la destrucción de elementos físicos del sistema o a la modificación de elementos lógicos, sino también a la manipulación y alteración de los datos que controla el sistema. El fraude informático produce o puede producir efectos dañinos en cualquiera de los tres ámbitos apuntados. Algunos de estos daños dejan intacta la propiedad física, como es el caso de la manipulación del programa de gestión de nóminas que proporciona un beneficio fraudulento para el defraudador sin ocasionar ningún daño físico al sistema.

2.8.1. PERJUICIOS PATRIMONIALES

Haremos referencia en este apartado a algunas formas de fraude informático y a las correlativas consecuencias dañosas para el patrimonio del afectado.

Por ejemplo en la consulta indebida de datos, la divulgación de una información confidencial puede traer graves pérdidas a las empresas. Si esta información es conocida por terceros extraños a la empresa o por la competencia las repercusiones económicas negativas para ésta pueden llegar a ser muy elevadas.

Otro ejemplo de fraude, la modificación de datos, también suele acarrear graves pérdidas económicas. En cuanto a la apropiación de datos, sin su destrucción o manipulación, también genera graves pérdidas económicas al contar la información, hoy en día, con un alto valor económico.

Por último la modificación de aplicaciones provoca, habitualmente, grandes beneficios para el defraudador y grandes pérdidas para la empresa o para el afectado.

2.8.2. AGRESIÓN A LA IMAGEN DE ENTIDADES FINANCIERAS

Los daños producidos por las acciones de fraude informático no se limitan al terreno material sino que con frecuencia transcienden al plano moral.

Entramos en este punto, aunque de un modo tangencial, en una cuestión

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ampliamente debatida en la doctrina y que hoy con base en la Declaración Universal de Derechos Humanos de 1948 y en la propia Constitución española de 1978 se reconoce casi con total unanimidad: el derecho al honor de las personas jurídicas. No debemos olvidar que en muchos de los supuestos fácticos de fraudes informáticos las víctimas son personas jurídicas. Pues bien, el derecho al honor, reconocido como fundamental en el artículo 18.1 de la Constitución Española, deriva de la dignidad humana (artículo 10.1 CE) y consecuentemente presenta, en su concepción estricta, un innegable carácter personalista. Ahora bien esto no excluye la extensión de su garantía constitucional a las personas jurídicas.

La jurisprudencia de nuestro Tribunal Supremo[129] admite reiteradamente la existencia y, por tanto, la protegibilidad del honor de las personas jurídicas. El Título I de la Constitución Española denominado "De los derechos y deberes fundamentales", no establece distinción entre personas físicas y jurídicas, de lo cual resulta que no son únicamente los derechos del individuo, en cuanto persona física, los tutelados. Por otra parte en diversos artículos de la CE se hace referencia expresa a las comunidades, confesiones, asociaciones, personas jurídicas, sindicatos, fundaciones, etc...

La explicación más clarificadora en este tema quizá sea la dada por la Sentencia del Tribunal Supremo de 15 de abril de 1992, en la que se distinguen los dos ámbitos en los que tiene ramificaciones el derecho al honor. Estas dos esferas del derecho al honor son la inmanente y la trascendente o exterior. La esfera inmanente del honor es difícil de atribuir a una persona jurídica, pero la exterior entendida como el derecho a gozar de una consideración pública sí es perfectamente atribuible a una persona jurídica.

Es precisamente esa consideración pública, el aspecto externo del honor de una persona jurídica el que puede verse afectado por una acción de fraude informático. Con este tipo de acciones se pone de manifiesto la vulnerabilidad

[129] Cfr. S. T.S. Sala 2ª 18 de febrero de 1981, ponente: Sr. Gómez de Liaño y Cobaleda. S. T.S. Sala 2ª 30 de abril de 1982, ponente: Sr. Hijas Palacios. S. T.S. Sala 4ª 7 de junio de 1989, ponente: Sr. Fuentes López. S. T.S. Sala 2ª 31 de octubre de 1980, ponente: Sr. García Miguel. S. T.S. Sala 1ª 15 de abril de 1992, ponente: Ortega Torres.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de la empresa, los fallos en sus sistemas de seguridad y como consecuencia de esto se genera una pérdida de confianza en la capacidad de la institución para desarrollar adecuadamente sus cometidos.

Las víctimas, que como anteriormente hemos dicho son fundamentalmente entidades bancarias y de seguros, suelen optar por resolver internamente el problema del fraude en sus sistemas informáticos. Además los perjuicios no afectan exclusivamente a la imagen pública de la entidad sino también a los propios empleados, responsables del proceso afectado por el fraude, que pueden ser acusados por la dirección de la empresa o por los clientes de no haber adoptado las medidas de prevención adecuadas.

En definitiva el daño moral a la imagen de la entidad repercute inevitablemente en el reconocimiento y prestigio profesional de los empleados directamente responsables del proceso informático afectado por el fraude.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3. FORMAS TÍPICAS DE FRAUDES INFORMÁTICOS

3.1. EXCLUSIONES

3.2. FORMAS TÍPICAS

3.2.1. AGRESIONES A LA INTIMIDAD PROVENIENTES DE ACCESOS ILEGALES A SISTEMAS INFORMÁTICOS, CON DERIVACIONES NEGATIVAS EN LA ESFERA PATRIMONIAL DE LA VÍCTIMA Y POSITIVAS EN LA DEL AUTOR

3.2.2. ESTAFA INFORMÁTICA DENTRO DEL ÁMBITO DE LA CONTRATACIÓN ELECTRÓNICA

3.2.3. FRAUDE EN LA TRANSFERENCIA ELECTRÓNICA DE FONDOS. PAGO ELECTRÓNICO. PAGO FRAUDULENTO MEDIANTE TARJETAS. PAGOS CON TARJETA EN INTERNET.

3.2.4. MANIPULACIONES DE SISTEMAS INFORMÁTICOS

3.2.4.1. MANIPULACIONES DE DATOS

3.2.4.1.1. MANIPULACIÓN DE LOS DATOS DE ENTRADA (INPUT)

3.2.4.1.2. MANIPULACIÓN DE LOS DATOS DE SALIDA (OUTPUT)

3.2.4.2. MANIPULACIONES DE SOFTWARE CON FINES FRAUDULENTOS

3.2.4.3. MANIPULACIONES DE CONSOLA (HARDWARE)

3.3. EL FENÓMENO INTERNET. FRAUDES EN LA RED

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3. FORMAS TÍPICAS DE FRAUDES INFORMATICOS

3.1. EXCLUSIONES

Es conveniente antes de adentrarse en la relación de acciones que pueden constituir fraude informático, recoger una enumeración negativa de aquellas conductas que pudiendo ser calificadas de ilícitos informáticos, y por su proximidad con el fraude, podrían confundirse con la figura del fraude informático.

En esta delimitación negativa es esclarecedora la exposición de Agustín Domínguez[130] que excluye del concepto de fraude informático las siguientes conductas: el hurto de software, hardware y datos, el robo de tiempo del ordenador, errores cometidos sin ánimo de engañar, destrucción del software o hardware y el acceso ilegal a sistemas informáticos sin intención de cometer fraude.

La exclusión de estas figuras delictivas de la categoría del fraude informático responde a una sencilla explicación: estos delitos no reúnen las características típicas del fraude. Siguiendo a Domínguez el fraude informático incluye tres aspectos fundamentales: la producción de un impacto financiero, la implicación del proceso electrónico de fondos en la perpetración o en el encubrimiento y la existencia en el autor de un ánimo de engaño[131].

Por tanto toda acción, aunque pueda calificarse de delictiva, si no reúne los elementos de acto intencionado de manipulación, ánimo de lucro y perjuicio o posible perjuicio de tercero no es calificable como fraude informático.

Si indudablemente este es un adecuado criterio delimitador de las conductas de fraude informático, tras la promulgación del nuevo Código Penal español debemos

---

[130] DOMINGUEZ, Agustín. *Transferencia Electrónica de Fondos y de Datos. Protección jurídica de los datos personales emitidos en una operación de pago electrónico.* En vol. Encuentros sobre Informática y Derecho 1992-1993. Coor. M.A. DAVARA. Aranzadi. Pamplona. 1993. Página 119 y ss.

[131] Cfr. punto 2.6 de este mismo trabajo.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

tomar, así mismo, como referencia la tipificación que del fraude informático se lleva a cabo a través del tipo de la estafa. El artículo 248.2 exige para la aplicación de este tipo: - ánimo de lucro en el autor,

- una manipulación informática y
- una transferencia de activo patrimonial inconsentida en perjuicio de un tercero.

3.2. FORMAS TÍPICAS

Debemos tener en cuenta que pretender establecer una enumeración exhaustiva de todos los tipos de fraudes informáticos es una tarea poco menos que imposible. El proceso de innovación tecnológica es constante, por tanto constantemente se desarrollan nuevas formas de falsear el funcionamiento normal de un sistema informático. Los fraudes informáticos, que aquí tratamos, son una de las muchas categorías de defraudación que se pueden dar dentro o fuera del seno de una empresa. Una clasificación general de fraudes dentro del ámbito empresarial en EE.UU es expuesta por Comer señalando las siguientes categorías: fraudes por quiebra, sobornos, fraudes informáticos, fraudes a consumidores, cheques y tarjetas de crédito, malversación, hurtos, receptación, fraudes en seguros y falsificaciones de valores.

Vemos por tanto cómo las empresas en la actualidad están sometidas a variadísimos riesgos y así se configura como uno de los objetivos empresariales el evitar en la medida de lo posible verse afectado por este tipo de riesgos. El riesgo del fraude, en el sentido de engaño, mentira, es uno de los más antiguos a los que se ven expuestas las empresas, y hoy viviendo como vivimos en una sociedad informatizada este riesgo de fraude es un riesgo informatizado. Esta situación de riesgo es percibida por los gestores de las empresas pero normalmente no se ve acompañada de una serie de medidas que prevengan eficazmente la comisión de estas conductas[132].

Teniendo en cuenta estos presupuestos hemos clasificado o agrupado en cuatro categorías las formas típicas[133] de fraudes informáticos.

---

[132] Véase en este sentido: HEVIA, Eduardo. *Procedimientos para luchar con el fraude en la empresa*. Estrategia Financiera, nº 51.

[133] Se utiliza la expresión "formas típicas" no en el sentido de formas delictivas tipificadas por la ley penal sino como conductas que

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3.2.1. Agresiones a la intimidad, provenientes de accesos ilegales a sistemas informáticos, con derivaciones negativas en la esfera patrimonial de la víctima y positivas en la del autor

Se está haciendo referencia aquí a un conjunto de conductas que entremezclan en el objeto de ataque tanto la agresión a la intimidad como el ataque al patrimonio de un individuo. No nos estamos refiriendo a esa parte de la delincuencia informática que afecta a la esfera de la intimidad de los individuos que ya el nuevo Proyecto de Ley Orgánica del Código Penal se encargaba de regular, en nuestra opinión, con gran acierto y que recoge el texto del nuevo Código Penal. Se trata de un conjunto de conductas que a través de un ataque a la intimidad de un individuo producen un perjuicio económico a éste y un beneficio al autor. Contamos con que el ánimo que mueve al autor es un ánimo de lucro y que el medio para la realización de esta conducta implica al proceso informático. Se trata de acciones con un doble objeto de ataque la intimidad y el patrimonio[134].

---

reúnen las características fijadas como comunes a los fraudes informáticos. Únicamente cabe hablar con rigor de forma típica de fraude informático a la nueva tipificación del delito de estafa recogida en el artículo 248.2 del Código Penal.

[134] Corresponde al legislador la tarea de precisar la forma de penalizar estas conductas. Sin pretender entrar en discusiones profundas de política criminal, estas conductas podrían constituir o bien delitos complejos o castigarse a través de la figura del concurso real de delitos. Los delitos complejos, como es el caso por ejemplo del robo con violación del art. 501 del anterior Código Penal, sólo representan un caso especial de concurso real de delitos del art. 69 del mismo Código que, por su altísima reprochabilidad el legislador quiso sancionar de una manera específica. Siguiendo con el ejemplo del citado artículo 501 en ese delito se producía una conjunción en un mismo ámbito de sendos ataques contra el patrimonio y contra la libertad de un individuo. Al hablar de un mismo ámbito nos referimos a un mismo ámbito espacio temporal. El delito complejo se rompería cuando entre una y otra acción, la de ataque al patrimonio y la de ataque a la intimidad en el caso que nos ocupa, se produce tal distanciamiento o disociación que cada infracción recobra por este hecho su autonomía. Por tanto puede defenderse la configuración de los ataques por medios informáticos a la intimidad con fines patrimoniales como delitos complejos considerando que la unión espacio temporal entre la agresión a la intimidad y la derivación de perjuicio patrimonial a la víctima, son coetáneas. Un ejemplo de estas conductas que venimos comentando lo constituiría una manipulación informática de datos personales como consecuencia de la cual se produce un beneficio económico para el autor y un perjuicio patrimonial a la víctima. Cfr. Sentencias del Tribunal Supremo de fechas: 29 de Enero de 1990; 28 de Noviembre de 1990 y

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3.2.2. Estafa informática dentro del ámbito de la contratación electrónica

Esta segunda agrupación de conductas corresponde ya exclusivamente a la delincuencia patrimonial o económica. La estafa informática, ya hemos visto, viene así tipificada en el nuevo Anteproyecto de Código Penal de 1994[135] y en el artículo 248.2 del vigente Código Penal. Se supera con esta nueva tipificación uno de los problemas que tradicionalmente ha presentado el tipo de la estafa para abarcar estas conductas que es la exigencia de un engaño "a otro", es decir, a otra persona.

Debemos tener en cuenta que la estafa informática puede afectar a dos ámbitos independientes: a las relaciones patrimoniales en general con independencia de la forma en la que se hayan constituido o generado y a aquellas otras relaciones económicas generadas por medios informáticos, la denominada contratación electrónica. En el primer grupo de estafas informáticas la informática juega un papel como simple medio de comisión de la conducta delictiva y en el segundo grupo los medios informáticos desempeñan una más amplia función: son medio para la conclusión de un contrato y son al mismo tiempo el medio para cometer una infracción, concretamente una estafa. Por tanto la estafa informática no se produce exclusivamente en el ámbito de la contratación electrónica sino en cualquier tipo de contratación aunque presenta un matiz diferencial cuando el engaño se produce en una relación configurada por medios electrónicos. En este tipo de contratación la relación de confianza iniciada o entablada con la relación contractual es aprovechada para la comisión de la estafa. En nuestra opinión estas son las conductas que realmente podrían calificarse como de fraudes informáticos. Como ya se expuso anteriormente, en los comentarios a la Jurisprudencia de nuestro Tribunal Supremo, es un elemento identificador del fraude la no necesidad del engaño y el aprovechamiento de una relación de confianza preexistente para

---

29 de Mayo de 1990.

[135] "Artículo 241.2. También se considerarán reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero." Anteproyecto de Ley Orgánica de Código Penal. 20 de mayo de 1994. Ministerio de Justicia e Interior.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

producir un error en otro que le induzca a la disposición patrimonial.

Sin duda podemos afirmar que una forma de contratación electrónica con un auge y expansión inimaginable hace pocos años es el comercio a través de la gran red Internet, el denominado comercio electrónico en Internet.

Dada la candente actualidad del tema permítasenos un breve análisis, desde un punto de vista jurídico, de algunos aspectos de una de las manifestaciones de la conclusión de contratos por vía electrónica y el cumplimiento de estos acuerdos a través del pago con tarjeta bancaria; el comercio electrónico a través de Internet.

Todos, sin duda, alguna vez nos hemos preguntado qué es, para qué sirve y hasta dónde puede llegar ese "monstruo" llamado Internet. Dar una respuesta completa a estas cuestiones excedería del objeto de este trabajo, por tanto centraremos la exposición partiendo de considerar Internet como una amalgama de miles de redes de ordenadores que conectan entre sí a millones de personas. A través de Internet y desde nuestro ordenador personal, dotado de un aparato llamado modem, (utilizando, por ejemplo, la línea telefónica) se pueden intercambiar ofertas comerciales con millones de potenciales clientes-consumidores en todo el mundo y a la inversa. Cada vez son más numerosas las entidades que facilitan servicios de comercio electrónico a través de Internet a sus clientes. Estos servicios crean **tiendas virtuales, Tiendas Internet, donde el usuario tras acceder a la información sobre los diferentes productos puede elaborar su pedido y realizar el pago mediante tarjeta de crédito**. Se ha descrito, brevemente, una operación de contratación electrónica en sentido estricto. Analizaremos a continuación las consecuencias que la legislación establece para este tipo de contratos.

Aspectos jurídicos del comercio electrónico.

Los servicios de comercio electrónico facilitados por entidades financieras no son sino operaciones de compra en las que se efectúa el pago electrónicamente. Desde la perspectiva de nuestro derecho positivo se

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

enmarcan estas operaciones en la denominada contratación entre personas distantes utilizando medios de comunicación. De acuerdo con la libertad formal que rige en el derecho contractual español (artículo 1.258 del Código civil) los contratos se perfeccionan por el mero consentimiento. Sin embargo si para la prestación de este consentimiento no media la presencia física de las partes, de acuerdo con lo dispuesto en el artículo 51 del Código de Comercio en referencia a la correspondencia telegráfica, para que produzca obligación entre los contratantes es necesario que éstos hayan admitido este medio previamente, y en contrato escrito, y que los telegramas reúnan las condiciones y signos convencionales establecidos con antelación. Por tanto, y utilizando como criterio interpretativo este artículo 51, la contratación utilizando correspondencia electrónica será válida entre aquellas partes que previo pacto hayan acordado que el medio electrónico y un determinado formato sea el soporte de sus respectivas declaraciones de voluntad. Aunque bien es cierto y siguiendo en este punto a autorizada doctrina, entre otros Díez Picazo, es posible la aceptación tácita de la utilización del medio electrónico produciéndose una vinculación en base a la inadmisibilidad del *venire contra factum proprium.* No encontramos así dificultad jurídica alguna en aceptar el medio electrónico como medio válido para la conclusión de contratos en derecho español pudiendo el **consentimiento producirse por la concurrencia electrónica de las voluntades de personas que previamente se han identificado**.

Identificación de los contratantes

Cabe aquí una pregunta a nuestro juicio clave ¿ES POSIBLE LA IDENTIFICACIÓN DE LOS CONTRATANTES QUE EMITEN SU CONSENTIMIENTO ELECTRÓNICAMENTE? Si el artículo 1.261 del Código Civil dice textualmente: "No hay contrato sino cuando concurren los requisitos siguientes: 1° Consentimiento de los contratantes ..." ¿cómo se puede hablar de consentimiento de los contratantes si no cabe una identificación electrónica previa de los mismos? (se entiende previa al consentimiento). En definitiva lo que se está planteando son las consecuencias de un vicio del consentimiento como es el error en la persona del otro contratante. De acuerdo con el artículo 1.266 del Código Civil el error en la persona sólo invalidará el contrato cuando la consideración a ella hubiere sido la causa principal de la contratación. Este artículo, según pacífica doctrina,

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

presume que por regla general la identidad de la persona no tiene en el derecho de la contratación un carácter esencial por lo que quien pretenda lo contrario debe soportar la carga de justificarlo y demostrar que el **contrato** se **realizaba *intuitu personae*.** Ahora bien una vez demostrado este extremo **la identificación del otro contratante se convierte en un problema jurídico de fondo** y no en un simple problema de prueba en relación a si existió o no suplantación por persona sin poderes expresos o tácitos de representación. En absoluto es esta una cuestión baladí ya que de cómo se resuelva la autentificación de los contratantes dependerá en definitiva la validez del mismo contrato.

Determinación del momento y lugar de celebración de un contrato entre personas distantes

Presentan máxima relevancia práctica el momento y lugar de celebración del contrato electrónico (por ejemplo en la determinación del Juez competente en los litigios que se susciten en la ejecución o cumplimiento del Contrato). Partimos de considerar que la formación del contrato se produce por la concurrencia electrónica de la oferta y la aceptación. La cuestión es determinar cuándo, cómo y dónde se produce esa concurrencia en operaciones de comercio electrónico. Sentencias del Tribunal Supremo de 28 de mayo de 1976 y 29 de septiembre de 1981 establecen dos reglas básicas: 1ª la declaración de aceptación es eficaz y perfecciona el contrato desde el momento que se reciba por el oferente, 2ª es eficaz la declaración de aceptación cuando una circunstancia imputable a culpa del oferente ha impedido su recepción. Para la determinación del *locus contractus* debemos acudir al inciso final del artículo 1.262 del Código Civil que establece que el contrato se presume celebrado en el lugar donde se hizo la oferta. Esta es una regla simplemente interpretativa prevaleciendo siempre lo pactado por las partes en contrato. Nos introducimos así en el ámbito de la convención entre las partes que en la determinación del marco jurídico del comercio electrónico y del intercambio electrónico de datos en general adquiere una relevancia especial dado que los aspectos hasta aquí expuestos parten de considerar operaciones de comercio electrónico nacionales, el problema se agrava si, como es lo más habitual, emisor y receptor se encuentran en distintos países con diferentes ordenamientos jurídicos. Consciente de esta problemática la COMISIÓN DE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

LA UNIÓN EUROPEA EN RECOMENDACIÓN DE 19 DE OCTUBRE DE 1994 propuso un MODELO EUROPEO DE ACUERDO DE EDI en el que se especifican los requisitos mínimos para el reconocimiento de validez jurídica a estos intercambios. Salvando las distancias entre los acuerdos EDI normalizados y las operaciones de comercio electrónico donde, en principio, no existe tal normalización, sí cabe destacar el artículo 6 de este modelo. En él se hace referencia a la seguridad de los mensajes de EDI y de él, así mismo, cabe extraer algunas conclusiones extrapolables a una operación de comercio electrónico.

Seguridad de los mensajes de EDI

Las partes que firmen el acuerdo de intercambio conforme con el modelo se comprometen a mantener unos procedimientos y medidas de seguridad que permitan: 1º la comprobación del origen, 2º la comprobación de la integridad, 3º el no repudio del origen y del destino y 4º la confidencialidad de los mensajes de EDI. Estas exigencias de seguridad hacen necesario el recurso a técnicas de criptografía en el tratamiento de los mensajes. No olvidemos que partimos de un supuesto de hecho como es el comercio electrónico en Internet donde el recorrido de un mensaje entre emisor y receptor es desconocido y los ataques a los que puede verse sometido ese mensaje son igualmente desconocidos.

Seguridad en los pagos en Internet

Ante las exigencias de seguridad referidas se están desarrollando estándares que cubran los cuatro puntos del referido artículo 6. Se basan estos estándares en la tecnología de cifrado asimétrico RSA protegiéndose así la confidencialidad, integridad de los datos y la comprobación del origen de la transmisión, pero cabría añadir la necesidad de la adopción de una tecnología que permita la identificación y autentificación de usuario.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En conclusión se puede afirmar la completa validez jurídica del contrato electrónico formalizado en una operación de comercio electrónico, es indudable el esfuerzo de todos los intervinientes (entidades y sociedades de medios de pago) por crear una seguridad que algunos califican de emocional y que creemos puede calificarse de real. No resta sino adoptar un medio de autenticación de usuarios, pues no son pocos los contratos que se quieren formalizar si, y solo si, la otra parte contratante queda autenticada con una palabra clave, con una llave y **con alguna característica propia de cada usuario,** medidas biométricas cuya incorporación a nuestras relaciones en el ciberespacio cabría reivindicar en orden a lograr una seguridad jurídica plena.

En el panorama descrito el fraude a través de la gran red podría producirse tanto desde el lado del comerciante que ofrece bienes o servicios inexistentes en la red, o suplanta el nombre y marca de un comerciante-proveedor de servicios real, como desde el plano del consumidor-usuario que "paga" utilizando números de tarjeta de crédito falsos o suplantando al verdadero titular del número de tarjeta utilizado[136]. Indudablemente los supuestos de hecho descritos quedarían abarcados por el nuevo tipo penal de la estafa[137] (art. 248.2 CP) puesto que al hablar, este artículo, de "alguna manipulación informática o artificio semejante", creemos permite penalizar la introducción de mensajes falsos en un *web site* de Internet induciendo a otros a realizar pagos (transferencias) con sus tarjetas por bienes o servicios inexistentes. A la inversa, la utilización fraudulenta de números de tarjetas para pagar bienes o servicios ofertados en la Red puede inducir a prestar o enviar esos servicios o bienes. En cualquier caso estas situaciones plantean, o pueden plantear, el grave problema de la ley penal aplicable cuando la acción delictiva se desarrolla en diversos países. La tipificación de los delitos varía de unos países a otros. Tomando como base de la acción delictiva una red con carácter

[136] En el siguiente punto se analizará cómo los esfuerzos técnicos en orden a evitar estas situaciones de fraude han alcanzado, y alcanzarán en un futuro inmediato, niveles de seguridad incluso superiores a las transacciones fuera del ámbito electrónico.

[137] "Lo que es ilegal fuera de la línea lo es también en línea." Comunicación de la Comisión de las Comunidades Europeas sobre *Contenidos ilícitos y nocivos en Internet*. COM (96) 487 final. Página 4.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

internacional como Internet aunque la legislación del país de la víctima penalice los hechos puede que el autor (suministrador de acceso a Internet, suministrador de contenidos, suministrador de servicios de ordenador central[138]) se encuentre fuera del alcance de las autoridades nacionales. Como regla general el Derecho Penal sólo es aplicable dentro del territorio nacional. Ante esta situación en la Unión Europea[139] ya se está estudiando la necesidad de armonizar las distintas legislaciones de los Estados miembros, en orden a establecer unos ciertos criterios mínimos comunes en la legislación penal en estos temas. Por tanto, aunque la legislación nacional existente es aplicable a Internet (art. 248.2 CP, estafa informática) se hace necesario alcanzar acuerdos en contextos más amplios no sólo a escala de acuerdos europeos, sino también, internacionales.

3.2.3. Fraude en la transferencia electrónica de fondos, (referencia a servicios de banca telefónica y banca electrónica). Pago electrónico. Pago fraudulento mediante tarjetas. PAGOS CON TARJETA EN INTERNET.

Fraude en la transferencia electrónica de fondos, (referencia a servicios de banca telefónica y banca electrónica)

Todos sabemos que con el advenimiento de la era de los ordenadores es

---

[138] La mayoría de los usuarios individuales de Internet no tienen un acceso directo permanente a la Red y, por tanto, pasan por un suministrador de acceso. De acuerdo el documento COM (96) 487 final de la Comisión de las Comunidades Europeas distinguimos los siguientes conceptos: - Suministrador de acceso a Internet: dan acceso a la red. - Suministrador de Servicios de ordenador central: permiten que el usuario albergue contenidos en un web (World Wide Web) el espacio en el que pueden visualizarse páginas con texto, gráficos, imágenes y sonido. - Suministrador de contenidos: cualquier usuario de Internet puede suministrar contenidos a la Red. Puede "hablar" o "escuchar". Así un receptor puede pasar a suministrador de contenidos propios, originales, o bien reexpedir los contenidos de un tercero.

[139] Cfr. ***Contenidos ilícitos y nocivos en Internet***. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Bruselas 16 de octubre de 1996. COM (96) 487 final.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

posible transferir grandes cantidades de dinero entre distintas ciudades o entre distintos continentes en pocos segundos con la transferencia electrónica de fondos.

Los usuarios de servicios de transferencia electrónica de fondos pueden utilizar en sus relaciones habituales con los bancos dos tipos de sistemas: aquellos sistemas denominados *on line* en los que se reciben y almacenan de modo instantáneo las operaciones realizadas por el cliente desde cualquier terminal. En los sistemas *on line* cada terminal está directamente conectado con el ordenador de la entidad financiera procesando inmediatamente, dicho ordenador, cada transacción que recibe de un terminal. Esta transacción es comprobada siendo atendida si existen suficientes fondos en la cuenta del cliente. Sin embargo en los sistemas *off line* la comprobación de las operaciones que han sido atendidas desde los distintos terminales se produce a posteriori. Cada terminal cuenta con un sistema de grabación donde quedan recogidas todas las operaciones realizadas desde dicho terminal en un determinado período de tiempo. Posteriormente estas operaciones, ya atendidas, son procesadas por el ordenador de la entidad financiera. Es fácil deducir de esta simplificada exposición que los sistemas *off line* son más vulnerables y están más expuestos al abuso.

Una manifestación de la Transferencia Electrónica de Fondos que hoy ya cuenta con un nivel de extensión, en cuanto a número de usuarios y entidades financieras prestadoras del servicio, muy alto son los denominados **servicios de banca telefónica y de banca electrónica**. Analizaremos a continuación la posible incidencia sobre los mismos de conductas de uso fraudulento y/o manipulación del sistema de acceso, así como, el sistema de reparto de responsabilidad ante estas incidencias diseñado por las entidades financieras prestadoras de dichos servicios.

Fraudes en servicios de banca telefónica y banca electrónica

Es cada vez más frecuente que al acercarnos a una sucursal bancaria solicitando la apertura de una cuenta o de una libreta casi sin darnos cuenta nos pongan delante un contrato de servicio de banca telefónica que ni hemos solicitado, ni puede que sepamos muy bien lo que ofrece y, desde luego, lo

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

que no sabemos es a lo que "su letra" nos obliga.

En las relaciones contractuales que consideramos, lejos de observarse el principio de la *libre autonomía de la voluntad* en virtud del cual en un contrato se establecen las cláusulas que ambas partes desean, el cliente se limita a adherirse a unas condiciones o cláusulas que sin posibilidad de modificación redacta la entidad que presta el servicio. Es decir nos situamos ante lo que se denominan las *condiciones generales de la contratación* que, en los contratos de banca telefónica, vienen a dar al traste con el justo equilibrio entre las partes contratantes. Estas *condiciones generales* en los contratos aludidos responden a una necesidad de colmar lagunas que el derecho positivo presenta en el sector de la distribución de los riesgos en estos servicios. No cabría objeción alguna si la distribución fuera equilibrada, sin embargo, el análisis de contratos de banca telefónica nos demuestra que las cláusulas abusivas respecto de la parte más débil de la relación (el consumidor) son habituales.

Así resultan muy frecuentes cláusulas limitativas de la responsabilidad de las entidades financieras que ofrecen estos servicios en relación con determinadas clases de riesgos como por ejemplo el riesgo de **fraude (utilización por terceros no autorizados)** y el riesgo de fallos técnicos.

En un cajón de sastre las entidades se autoexoneran de responsabilidad en el funcionamiento de estos servicios a través de cláusulas del siguiente tenor: "... la entidad no se hace responsable de cualquier fallo, error técnico, accidente, avería, manipulación, interrupción del servicio o cualquier otra incidencia que pudiere surgir, por incorrecta instalación, o deficiente mantenimiento, en los servicios técnicos ajenos a la entidad y cuyo uso sea necesario para la utilización del servicio", "el titular del servicio acepta y admite, en todo caso, cualquier operación que se haya realizado mediante la utilización del número de identificación personal aun en el supuesto de que haya sido realizado por tercera persona no autorizada..."[140].

Los riesgos de fraude aludidos se producen como consecuencia de la pérdida, sustracción o utilización indebida de las claves de acceso y seguridad que tiene

[140] Estipulaciones cuarta y quinta del contrato del servicio TELECAM de Caja de Madrid.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

el titular del servicio de banca telefónica. En el origen de los posibles fraudes se encuentra el hecho de que los sistemas de acceso al servicio de banca telefónica no garantizan en términos absolutos la identidad del usuario y el resto de los aspectos de la seguridad de las órdenes verbales. Ordenes que pueden consistir en transferencias, traspasos entre cuentas asociadas al servicio, etc...

El control de acceso implementado en la mayoría de los servicios de banca telefónica y banca electrónica se basa en la identificación por clave y número de identidad del Usuario. Indudablemente es un sistema económico en su mantenimiento para la entidad. En él, el usuario debe teclear (banca electrónica) o transmitir vía voz (banca telefónica) su clave e identidad. El coste de explotación de poner en marcha el sistema se limita a los costes de comunicación de estas claves y su renovación periódica. Hay algún contrato, en lo que sin duda podemos calificar de uso abusivo del lenguaje, que califica de firma electrónica a un medio adicional de identificación consistente en una tabla numérica. Esta tabla está formada por un entramado de filas y columnas con números en cada recuadro formado por la intersección de esas filas y columnas, la entidad requiere aleatoriamente al usuario, de acuerdo con unas coordenadas, cualquiera de esos números antes de cada operación. Decimos que es uso abusivo del lenguaje calificar este sistema como firma electrónica pues el concepto de firma electrónica tiene ya contornos definidos no sólo técnicamente sino también desde un punto de vista normativo en leyes recientes como la del estado de Utah (Utah Digital Signature Act[141]) o en nuestro entorno geográfico la ley alemana sobre firma electrónica o digital. Sobre la base de uso de un criptosistema asimétrico de clave pública se genera una firma digital propia de cada usuario a la que las leyes mencionadas atribuyen los mismos efectos que a la firma de puño y letra sobre papel. La firma electrónica se basa en la encriptación de mensajes, posible en banca electrónica pero no en banca telefónica (el terminal telefónico es unidireccional y los mensajes no son susceptibles de encriptación) que es donde precisamente algunas entidades en el contrato de uso del servicio utilizan el concepto.

[141] Utah Digital Signature Act Utah Code Annotated Title 46, Chapter 3 (1996).
Texto de la ley disponible en Internet http://www.state.ut.us/ccjj/digsig/dsut-act.htm

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Como alternativas posibles al control de acceso a través de claves (passwords) se barajan diversas soluciones por los expertos. Dando un paso más en la identificación del usuario ésta cabría efectuarla no sólo por lo que sabe (claves-passwords), sino también por algo que tiene. Por ejemplo tarjeta de banda magnética tradicional, tarjeta con *chip* electrónico o a través de un disquete propio de usuario[142]. Este último sistema sería el de menores costes de implantación ya que el disquete es un dispositivo de almacenamiento externo de datos de extensa utilización, y cualquier PC dispone de un periférico de lectura-escritura adecuado para interpretar los datos del disquete. Indudablemente la identificación con tarjeta con *chip* electrónico presenta una ventaja fundamental frente a los otros sistemas propuestos como es la dificultad para duplicarla y la autonomía del propio instrumento para realizar chequeos, validaciones, cifrado de información. Como desventaja se cita la necesidad de un elemento hardware conectado al ordenador del usuario sensiblemente más caro que una unidad de lectura de disquetes. Incorporar un dispositivo de lectura de tarjetas a un terminal telefónico supondría unos costes muy por encima de los razonablemente asumibles, sin embargo, en banca electrónica la identificación a través de disquete parece un incremento de seguridad posible.

Por tanto si en un lado de la balanza nos planteamos un incremento de la seguridad posible técnicamente y en el otro situaciones en que se ven afectados los fondos depositados en la/s cuenta/s corriente/s asociada/s, es justo abogar por un equilibrio.

En orden a determinar las responsabilidades de una orden no autorizada por el titular del servicio es fundamental atender a la naturaleza jurídica de la cuenta/s sobre la que en definitiva tienen su reflejo las órdenes telefónicas. El depósito bancario de dinero en cuenta corriente, es un contrato *sui generis* y complejo que, con independencia de las liquidaciones periódicas necesarias para la determinación del saldo exigible previa conformidad de las partes, obliga al deudor a devolver dicho saldo. Esta obligación según **el Tribunal Supremo** tiene carácter casi absoluto. Dice el alto Tribunal: ***"La obligación de conservación y devolución, que tanto el Código de Comercio como el Código***

[142]BIELZA LINO, Cristóbal. *"El disquete como alternativa a las tarjetas de crédito para dar seguridad a las transacciones en InfoVía e Internet"*. Libro de Ponencias del II Congreso Nacional de Usuarios de Internet e Infovía. 4 al 6 de febrero de 1997. Madrid.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Civil imponen al depositario, tiene carácter casi absoluto, y sólo decae mediante una causa muy justificada de fuerza mayor o de caso fortuito, no previsible ni evitable. Ello lleva a exigir la ***responsabilidad de la entidad bancaria*** *por los menoscabos, daños y perjuicios que el demandante haya sufrido por su negligencia".*

Asimismo el depósito en cuenta corriente bancaria se caracteriza principalmente por la obligación que asume el Banco de efectuar el servicio de caja. Dentro de este servicio de caja se incluyen todos los cobros y pagos realizados por el banco como comisionista del titular de la cuenta corriente. Si el banco tiene la condición de depositario y comisionista y, como tal, no puede actuar contra disposición expresa del cliente difícilmente cumplirá con su obligación si el sistema que implanta para atender órdenes sobre cuentas corrientes, y otros productos de pasivo, no permite identificar al titular de la cuenta.

En este sentido resulta de máximo interés una Sentencia de la Audiencia Provincial de Ciudad Real (Sección 2ª) que, en relación con otro servicio automatizado como es el de cajeros dice textualmente:"*... lo cierto es que el usuario no se identifica ante el cajero automático, limitándose a digitaliza la clave numérica personal."*

En definitiva ¿qué consecuencias se derivan de esta falta de identificación del usuario de banca telefónica?

Vuelve a ser la jurisprudencia de las Audiencias la que de forma clara y precisa establece que: **"... era OBLIGACIÓN INDISPENSABLE la de identificar al titular, y este hecho corresponde acreditarlo a la entidad depositaria, al ser un HECHO EXTINTIVO de su responsabilidad, como exige el artículo 1214 del Código Civil .... con lo que aparece con nitidez la omisión de diligencia constitutiva de la CULPA CONTRACTUAL, y que obliga a la entidad financiera demandada a indemnizar los daños y perjuicios causados**, es decir las sumas reclamadas más sus intereses, de conformidad a lo que dispone el Código Civil".

Es decir, es sobre la entidad sobre la que recae la carga de probar que identificó al titular del servicio para así exonerarse de responsabilidad en una

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

operación no autorizada por éste. En este sentido la **Audiencia Provincial de Granada** tiene declarado que: "... la responsabilidad del demandado no nace del hecho del robo o hurto de la libreta de ahorros, pues este hecho por sí solo no hubiera desencadenado los efectos producidos si la referida entidad hubiera cumplido su anexa obligación de identificar al titular de la libreta, lo cierto es que dicha cláusula exoneratoria es inoperante, ya que tratándose de un contrato de adhesión el de autos, sus condiciones generales caen bajo la normativa de la **Ley General para la Defensa de los Consumidores y Usuarios, de 19 de julio de 1984**, al tratarse el actor de un consumidor final, y en concreto incurre en la **nulidad** prevista en el **art. 10.4** de la citada Ley, en relación con lo establecido en el apartado 6 de la letra c) del número 1 de dicho precepto, que establece la exclusión de aquellas cláusulas que contengan limitaciones absolutas de responsabilidad frente al consumidor o usuario".

No existe aún una jurisprudencia específica en esta materia de banca telefónica, dada su todavía reciente implantación, pero de lo que no cabe duda es de que el titular de un servicio de banca telefónica no se encuentra protegido por el contrato de dicho servicio. Habrá de acudirse a las normas del ordenamiento[143] y a una jurisprudencia que como hemos visto se muestra marcadamente tuitiva de los intereses de los clientes ante lo que sin duda se pueden calificar de cláusulas abusivas en la contratación.

[143] El artículo 8.3 del Real Decreto 629/1993, de 3 de mayo, sobre Normas de actuación en los Mercados de Valores y Registros obligatorios, y la Circular de la Comisión Nacional del Mercado de Valores 3/1993, de 29 de diciembre, admiten que el archivo de justificantes de órdenes de compra, venta, suscripción y reembolso de valores, etc... dadas por vía telefónica se realice en cinta de grabación y si se efectuaron dichas órdenes por vía electrónica el soporte de almacenamiento sea un registro magnético. Pero lo más importante es que este artículo 8.3 establece claramente los requisitos mínimos jurídicamente exigibles para poner en funcionamiento un servicio telefónico dentro del ámbito del mercado de valores, en concreto: *"Aquellas entidades dispuestas a aceptar órdenes recibidas por vía telefónica no escrita deberán establecer los medios necesarios para la **identificación de sus ordenantes**, así como disponer de cintas para la **grabación de dichas órdenes**; siendo necesario, no obstante, advertir previamente al ordenante de dicha grabación. Será necesaria, asímismo, la existencia de **confirmación escrita** de la orden por parte del ordenante, siendo admisible la utilización de cualquier medio escrito tales como télex, fax u otros similares"*. La falta de esta confirmación escrita, a que se hace referencia en este artículo, tiene como único efecto el incumplimiento de una norma administrativa, por lo que no afecta a la validez sustantiva y eficacia mercantil de la orden. No olvidemos que en derecho español rige, como principio general, la libertad de forma.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Junto a las cuestiones apuntadas revisten una importancia jurídica máxima la validez jurídica y eficacia probatoria de las transacciones efectuadas a través de estos servicios de banca telefónica y banca electrónica.

Esta nueva forma de operar lleva aparejada una serie de exigencias. Exigencias que pueden concretarse en garantía de la identificación plena del cliente, validez o eficacia jurídica de las operaciones contratadas, prueba magnética de las mismas con plenos efectos procesales ante posibles controversias, un reparto equitativo de responsabilidades por daños y perjuicios ante supuestos de fraude o fallos operativos de los sistemas informáticos y, como no, el cumplimiento de la normativa específica para entidades de crédito sobre transparencia de las operaciones y protección de la clientela.

En relación con la validez probatoria de las grabaciones de las conversaciones de banca telefónica caben las siguientes consideraciones[144].

La constatación de la operación efectuada se suele resolver en los contratos de uso del servicio de banca telefónica a través de una cláusula por la que el usuario autoriza expresamente a la entidad para grabar magnetofónicamente en su integridad las conversaciones telefónicas de utilización del servicio aceptando, así mismo, su valor probatorio. La obtención de estas pruebas respeta las reglas de la buena fe, como expresamente exige el artículo 11.1 de la Ley Orgánica del Poder Judicial[145], siendo calificable de lícita. No obstante dado que la obtención y conservación de las grabaciones tiene carácter unilateral (por una de las partes del contrato, la entidad) deben adoptarse medidas de seguridad en el archivo y custodia de las mismas. La entidad debe garantizar la integridad y no manipulación de los soportes de la grabación, si no, en un procedimiento judicial la entidad puede encontrar que de contrario

[144] Cfr. MATEU de ROS, Rafael. *"La Contratación Bancaria Telefónica"*. Revista de Derecho Bancario y Bursátil. Año XV. Abril-Junio 1996, nº 62. Página 265 y ss.

[145] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Artículo 11.1. En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

se alega la no realización de la operación o, al menos, no en los términos que se desprenden de la grabación efectuada en un soporte manipulable.

Centrándonos ahora en banca electrónica la utilización en estos servicios de sistemas de firma digital dotaría de plena fuerza probatoria y validez jurídica a las operaciones firmadas electrónicamente. Con ello no solo se garantiza la identificación de las partes sino también la integridad, confidencialidad y no repudio de los mensajes emitidos. Lo que parece aventurado es un sistema de banca electrónica en el que los mensajes, entre usuario y entidad, viajen en claro por la red de comunicación o donde el único sistema de identificación de acceso al servicio sean unas claves tecleadas desde el ordenador personal del usuario. Si a este sistema se añade una cláusula, en el contrato marco entre entidad y cliente, en la que éste acepta como válidas y correctas todas las operaciones cursadas mediante el uso de las mencionadas claves creemos que no cabe por menos que traer a colación la sentencia de la Audiencia Provincial de Sevilla de 30 de julio de 1992, que declaraba nula la cláusula (en ese caso en un contrato de uso de tarjeta) en la que el consumidor daba por buenas las transacciones recogidas en el cajero automático al vulnerarse el artículo 24 de la Constitución Española, el 1.214 del Código Civil y el 10.4 de la Ley General para Defensa de los Consumidores y Usuarios. Es evidente que sobre un sistema sobre el que la seguridad técnica presente importantes agujeros no cabe el establecimiento de cláusulas de exoneración de responsabilidad de la entidad.

Por último, y en lo que respecta a la aplicabilidad a la contratación (operaciones de activo o de pasivo) desarrollada a través de banca electrónica y telefónica de la normativa financiera específica de entidades de crédito (OM de 12 de diciembre de 1989 y Circular 8/1990 del Banco de España[146]) cabe

[146] Esta normativa trae causa del desarrollo del artículo 48 de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito. Este artículo 48 faculta al Ministerio de Economía y Hacienda para que *"con el fin de **proteger los legítimos intereses de la clientela activa y pasiva de las entidades de crédito** y sin perjuicio de la libertad de contratación que, en sus aspectos sustantivos y con las limitaciones que pudieran emanar de otras disposiciones legales, deba presidir las relaciones entre las entidades de crédito y su clientela, pueda: a) Establecer que los correspondientes **contratos se formalicen por escrito** y dictar las normas precisas para asegurar que los mismos **reflejen de forma explícita y con la necesaria claridad los compromisos contraídos por las partes y los derechos de las mismas ante las eventualidades propias de***

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

decir que se exige un documento contractual escrito en todo caso. Esto no debe entenderse que afecta a la validez y eficacia de la contratación verbal a través de teléfono, la exigencia de un contrato escrito es un requisito que cabe cumplir bien de forma previa, con la firma del contrato marco de uso del servicio de banca telefónica o electrónica, o bien posteriormente en contrato independiente. Lo que sí se desprende de la normativa estudiada es la exigencia de un sistema de constatación de las operaciones formalizadas por vía telemática que revele la autoría, la intención contractual de las partes y el contenido esencial del contrato. Para cubrir estas exigencias de seguridad jurídica creemos adecuada la firma digital o electrónica que incorporada a un mensaje emitido a través de banca electrónica dota a éste de autenticación e irrefutabilidad de origen y recepción e integridad de contenido.

Fraude en pagos electrónicos. Pagos fraudulentos con tarjetas

La casuística en relación con la utilización abusiva e irregular de los cajeros automáticos es muy amplia[147] y ya se expuso con anterioridad, por tanto no se reincidirá sobre el tema[148]. Parte de la doctrina entiende que únicamente un

---

cada clase de operación...". Queda claro, a la luz de la norma transcrita, que la infracción del requisito de la formalización por escrito es una infracción de una norma de disciplina de entidades de crédito que, en modo alguno constituye una sanción de nulidad del contrato en sí. Es decir, el artículo 48 transcrito se remite al principio general de la libertad de forma. Siendo esta la interpretación que consideramos como más adecuada, siguiendo así a MATEU DE ROS op. cit., lo que sí cabe deducir es una exigencia ineludible para toda entidad de crédito de contar con un sistema que permita la comprobación de la voluntad contractual de las partes y del contenido del contrato. No necesariamente ha de ser un sistema de escritura en soporte papel con firma de puño y letra de las partes, un documento en soporte electrónico con firma digital llena las exigencias jurídicas indicadas.

[147] Una clasificación muy completa de las irregularidades que se pueden cometer en relación con los medios electrónicos de pago es la recogida por E. Del Peso en su ponencia *El fraude en los medios electrónicos de pago*, publicada en vol. Encuentros sobre Informática y Derecho 1992-1993, ICADE. Aranzadi. Pamplona 1993. Página 161 y ss.

[148] Recordamos la clasificación propuesta por Emilio Del Peso, Op. Cit. que divide las irregularidades cometidas en relación con los medios electrónicos de pago en cuatro grandes grupos: irregularidades cometidas por los titulares de las tarjetas, irregularidades cometidas por terceros, cometidas por los prestadores de servicios y las cometidas por las entidades emisoras y/o gestoras de las tarjetas.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

solo conjunto de este tipo de conductas **constituyen fraude informático**. Se trata de aquellas actuaciones en las que se tiene **acceso a un cajero automático mediante la utilización de una tarjeta falsa**. El uso de una tarjeta falsificada reúne todas las características del fraude al constituir precisamente esta falsificación el elemento del engaño necesario en todo fraude. Para Bueno Arús[149] la utilización de este tipo de tarjetas tiene calificación equivalente, ya se utilicen para comprar en el comercio o para obtener dinero de un cajero automático. Sin embargo Romeo Casabona[150] entiende que la utilización de este tipo de tarjetas falsificadas únicamente puede llegar a tener éxito en establecimientos comerciales donde no se proceda a la comprobación de la identidad del tenedor de la tarjeta. Ambos autores coinciden, no obstante, en la calificación jurídica de estos hechos entendiendo que se produce un concurso entre el delito de falsedad en documento y el delito de estafa.

Descendiendo ahora a la casuística en relación con la falsificación de tarjetas cabe hacer las siguientes consideraciones con base en investigaciones efectuadas sobre casos reales aparecidos en prensa[151] y en las memorias anuales publicadas por la Dirección General de Policía, en concreto la estadística de criminalidad accesible en el INE (Instituto Nacional de Estadística).

Al desarticular las redes de falsificadores, en definitiva, al desmontar estos fraudes se toma conciencia de la inseguridad de un sistema de disposición de efectivo y pago que todos habitualmente utilizamos.

En un estudio de campo con los responsables de redes de cajeros, policía y departamentos de reclamación de bancos y cajas se presenta el siguiente panorama.

Actualmente los datos conocidos de fraudes con tarjetas bancarias representan

[149] BUENO ARUS, Francisco. Op. Cit. Pág. 5.

[150] ROMEO CASABONA, Carlos María. Op. Cit. Pág. 135.

[151] Una de las últimas noticias aparecidas en prensa sobre falsificación de tarjetas de crédito es la publicada por el periódico EL PAIS el miércoles 4 de diciembre de 1996.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

un porcentaje mínimo de los realmente cometidos. Los fraudes conocidos se concentran fundamentalmente en dos apartados: **uso de tarjetas extraviadas o robadas (tarjetas calientes** que comprende el 80% de los datos conocidos) y **falsificación de tarjeta** (abarca el 20% restante).

La utilización de tarjetas calientes (substraídas o extraviadas) por terceros es sencilla en comercios, si no se comprueba la identidad del usuario de la tarjeta ni se exige el NIP. Es excepcional que los comerciantes comprueben la identidad del portador de la tarjeta, consumidor de un bien o un servicio. Además, en ocasiones, ni siquiera se firman los justificantes de compra, no produciéndose el cotejo de firmas que evitaría numerosos usos fraudulentos de tarjetas.

Para que sea posible la utilización fraudulenta de tarjetas calientes en cajeros automáticos es necesario, por parte de los defraudadores, una mayor y más consolidada infraestructura para la obtención de los NIP (Números de Identificación Personal) excepción hecha de la obtención del NIP por visualización directa. En concreto algunos de los métodos utilizados para la obtención del NIP consisten en la instalación de cámaras de video ocultas en los mismos cajeros automáticos enfocadas hacia el teclado donde el usuario introduce desprevenidamente su NIP[152]. Una vez obtenido éste la tarjeta e substraída a su titular. De la casuística expuesta cabría deducir que son posibles disposiciones efectuadas desde cajero con uso del NIP sin que pueda apreciarse una custodia negligente de este número por parte del titular.

Junto a los usos fraudulentos de tarjetas "calientes" se encuentra otro grupo de actuaciones fraudulentas con tarjetas, **las falsificaciones**. En la práctica se han detectado dos formas de comisión: la falsificación integral de la tarjeta (alto coste) para su uso posterior en comercios y la manipulación de tarjetas robadas recodificando su banda magnética. En este último caso la banda magnética de una tarjeta ya anulada (o incluso un plástico blanco con banda magnética), es recodificada con datos de una tarjeta en circulación. Estos datos son obtenidos

[152] Otra forma de obtención de Números de Identificación Personal ha sido la colocación de una cinta invisible (transparente) sobre el teclado del cajero donde queda señalado el número tecleado por el usuario y que, posteriormente, al retirar la cinta puede leerse dicho número por el delincuente.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

a través de los más pintorescos métodos por ejemplo: en establecimientos, donde momentáneamente se pierde de vista la tarjeta, un empleado infiel decodifica los datos de la tarjeta; sustitución del sistema de apertura del recinto que alberga el cajero automático por un lector de banda magnética instalado por los defraudadores. El terminal punto de venta (TPV) del establecimiento sólo lee los datos codificados en la banda que pertenecen a tarjetas activas autorizándose por tanto la operación. En los supuestos mencionados de plásticos blancos con banda magnética recodificada con datos de tarjetas en circulación, la dinámica comisiva del delito exige connivencia entre defraudador y comercio, desde donde se utiliza el plástico.

Dada la trascendencia social de las conductas que estamos estudiando el **nuevo Código Penal**, reflejo del orden valorativo de una determinada sociedad, tipifica el uso abusivo de tarjetas electrónicas.

Los hechos descritos dan lugar a situaciones penalizables con arreglo a dos tipos fundamentalmente: robo (arts. 238 y 239) o estafa (art. 248.2). Parte de la doctrina entiende como más adecuada la tipificación como delito de robo con fuerza en las cosas la utilización de tarjeta legítima por un tercero. De acuerdo con el artículo 238 del nuevo Código penal: *"Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:*

(...)
4º Uso de llaves falsas".

El artículo 239[153] explicita el concepto de llave falsa diciendo: *"Se*

[153] El nuevo Código Penal con este artículo 239 ha zanjado una cuestión que había sido objeto de discusión por la doctrina y jurisprudencia. El T.S. sostenía, antes de la promulgación del nuevo C.P., que las tarjetas de crédito tenían la consideración de llaves. Así el Alto Tribunal en Ss de 5 de noviembre de 1987; 6 de marzo de 1989; 27 de febrero y 21 de septiembre de 1990, entre otras, declaró que las tarjetas tienen el carácter de llaves "por cuanto sirven en la práctica para accionar el cierre del local que da acceso al cajero automático, o para abrir el receptáculo del mismo cuando se halla instalado en el exterior del establecimiento bancario". Añadía el T.S. que "dicho carácter de llave no se desvirtúa por el hecho de que tenga atribuida una segunda función: la de servir para extraer dinero pulsando el número secreto, porque la acción típica está cumplida con la simple apertura del espacio cerrado. Si el número secreto no se conoce la acción de obtener dinero quedará en

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

considerarán llaves falsas:

(...)

2º Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.

(...)

A los efectos del presente artículo, se considerarán llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia".

De acuerdo con los artículos transcritos entendemos que son aplicables al uso de tarjetas legítimas substraídas si no se ha producido ninguna manipulación sobre dichas tarjetas. Sin embargo en el uso de tarjeta falsificada se aprecia un plus de desvalor[154], como es el engaño a la entidad depositaria de los fondos y al titular del instrumento de pago. Es la utilización de esta tarjeta falsificada la que constituye una manipulación del "input", y por tanto una de las formas del delito de estafa penalizadas a través del artículo 248.2 del nuevo Código Penal, consiguiendo la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

PAGOS CON TARJETA EN INTERNET

La casuística de fraudes con tarjetas se ha ampliado con la utilización de éstas en los pagos de bienes o servicios adquiridos a través de Internet. Un análisis jurídico de las operaciones de comercio electrónico en la Red obliga a adoptar una doble perspectiva: civil y penal. Desde la primera deben ser analizados los derechos de los consumidores en contratos negociados a distancia[155]. Y desde

---

grado imperfecto de ejecución".

[154] Este incremento del desvalor de la conducta de uso de tarjeta falsificada se traduce en la mayor pena del delito de estafa fijada en el artículo 249 en prisión de seis meses a cuatro años, pudiendo llegar hasta seis años si concurren determinadas circunstancias. El artículo 240 castiga el delito de robo con fuerza en las cosas con pena de prisión de uno a tres años, pudiendo llegar hasta cinco años de prisión si el robo se comete mediando alguna de las circunstancias del artículo 235.

[155] Cfr. nota al pie número 92.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

la segunda, las consecuencias penales del uso fraudulento de tarjetas de crédito en Internet. Nos centraremos en este segundo aspecto.

Sin duda se están realizando importantes avances en la seguridad de los mensajes que circulan por la red mundial Internet. Quizá en buena parte estos avances han venido propiciados por la utilización de esta red de redes en el ámbito comercial. La circulación de datos con un alto valor económico y la realización de transacciones exige una garantía de inviolabilidad de la transmisión que la técnica puede proporcionar.

De acuerdo con la legislación interna, Ley del Comercio Minorista, el consumidor queda indemne ante un cargo efectuado utilizando el número de su tarjeta de crédito. Efectivamente esto es así ya que el protocolo de seguridad que hasta ahora se ha utilizado (SSL) permite que la información viaje cifrada, se identifica a la tienda pero no al otro extremo de la transmisión, el comprador. Por esta razón se firma entre entidad y comerciantes que realicen ventas por teléfono y ventas en Internet un mismo régimen donde toda responsabilidad ante posibles incidencias se hace recaer sobre el comerciante. Con ello la responsabilidad civil derivada de una conducta indudablemente delictiva se hace recaer precisamente sobre el perjudicado, víctima del engaño. Sin embargo la situación ha cambiado, y aún experimentará una mayor evolución en un futuro inmediato. Las grandes marcas de tarjetas ya han desarrollado el protocolo SET (Transacciones Electrónicas Seguras) para securizar los pagos con tarjeta en redes abiertas como Internet. Con SET podemos decir que los niveles de seguridad en las transacciones en el mundo real se llevan al mundo virtual, electrónico. En otras palabras, igual que al acercarnos a un comercio y pagar con nuestra tarjeta firmamos un comprobante de la compra, en las compras que hagamos en Internet también firmaremos un comprobante. Será una firma electrónica que basada en sistemas de encriptado asimétrico permite identificar electrónicamente al extremo de la transacción en la que supuestamente se encuentra una determinada persona, el comprador. Conviene resaltar cómo hacemos mención a la identificación electrónica del extremo, pero no a la autenticación del comprador. Hemos conseguido quedar identificados en el mundo electrónico como entes existentes y legitimados para llevar a cabo un pago o una transacción, pero ¿cómo nos identificamos como persona autorizada que lleva a cabo una determinada operación?. Para ello Europay, MasterCard y Visa

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

pretenden incorporar al ámbito del comercio electrónico la tecnología de las tarjetas con "chip" (EMV). La fusión del protocolo SET y de EMV, que se espera se encuentre disponible para el tercer trimestre del año 1997, dará un paso más en orden a cerrar el círculo de compras electrónicas seguras que conllevará un inevitable cambio en el reparto de responsabilidades ante incidencias[156]. Se podrá probar que un determinado titular de tarjeta ordenó un determinado pago. Así la constatación de que una compra ha sido efectivamente realizada por el titular de una tarjeta llevará a todos los intervinientes (consumidores, comercios y entidades) a reducir ostensiblemente su nivel de riesgo en pagos electrónicos. El descubrimiento y prueba del autor de un delito de estafa informática por utilización fraudulenta de tarjeta de crédito en Internet será posible en un futuro inmediato.

3.2.4. Manipulaciones de sistemas informáticos

Las manipulaciones de los sistemas informáticos son las formas más frecuentes de aparición de la criminalidad informática. Las manipulaciones más frecuentes de los sistemas informáticos son las manipulaciones de datos. En estas manipulaciones el autor buscando un lucro personal modifica una ser[illegible] de datos a los que tiene acceso por razón de su puesto de trabajo o p[illegible] cualquier otra circunstancia personal. La sustitución del dato correcto por e[illegible] manipulado constituye el elemento del engaño necesario en el fraude. Casi todas las conductas enjuiciadas en las Sentencias de nuestro Tribunal Supremo recogían como hechos probados manipulaciones de datos a consecuencia de las cuales se habían percibido indemnizaciones indebidamente, o se cobraban prestaciones a las que no había derecho a la vista de los datos ciertos de los autores de la manipulación. Para comprender un poco mejor cómo se

[156] IDENTIFICACIÓN DEL ORDENANTE DE UN PAGO CON TARJETA EN INTERNET

Estándar de comunicación / Elementos de identificicación	SSL	SET	SET-EMV
TARJETA	NO	NO	SI
CLAVE	NO	SI	SI
FIRMA	NO	SI	SI
CARACTERÍSTICA PERSONAL	NO	NO	SI

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

producen este tipo de manipulaciones debemos partir de considerar al ordenador como un sistema integrado para el proceso de datos. El proceso de datos supone la existencia de unos datos de entrada (input), la existencia de unas órdenes que guíen las operaciones a realizar con dichos datos (un programa) y unos datos que constituyan el resultado de la aplicación a los datos de entrada de las órdenes o instrucciones del programa (output). Quedan así recogidos los tres puntos donde puede tener lugar la incidencia de la manipulación del sistema informático: en el input, en el programa o en el output.

3.2.4.1. Manipulaciones de datos

3.2.4.1.1. Manipulación de los datos de entrada (input)

Las manipulaciones de los datos de entrada generalmente son cometidas por los responsables de controlar la entrada de datos en el sistema. Su situación privilegiada dentro del proceso de datos les facilita sobremanera la realización de la conducta engañosa[157]. Las manipulaciones de este tipo suelen producirse en sistemas que generan pagos automatizados. La introducción de controles en estos sistemas de pagos automatizados es imprescindible. Podría resultar de utilidad en este sentido la realización de sucesivos cuadres contables a medida que se van introduciendo nuevos datos en el proceso informático.

3.2.4.1.2. Manipulación de los datos de salida (output)

Dentro de este grupo se incluyen todas las modificaciones de los datos resultado del proceso informático. Por ejemplo una

[157] A este respecto ya hemos señalado cómo el artículo 250.1.7°, del nuevo Código Penal, establece una pena agravada para el delito de estafa, concretamente pena de prisión de uno a seis años y multa de seis a doce meses, cuando el delito se comete con abuso de las relaciones personales existentes entre víctima y defraudador, o aprovechando éste su credibilidad empresarial o profesional.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

modificación de los listados obtenidos del ordenador con los resultados correctos. La manipulación no se produce ni en los datos de entrada, ni en el proceso ya que éste da unos datos correctos, la modificación la sufren unos datos ciertos que posteriormente son falseados.

3.2.4.2. Manipulaciones de software con fines fraudulentos

Dentro de las denominadas manipulaciones del programa[158] o manipulaciones del software se incluyen dos tipos de conductas: aquéllas en las que el autor modifica los programas de la empresa o del particular afectado, y aquellas otras modificaciones que se producen con la ayuda de un programa que ha creado el propio delincuente.

En este tipo de fraude la acción delictiva consiste en trastocar el proceso de cálculo del programa de forma que en un determinado momento o bajo unas determinadas condiciones, el programa no actúe conforme a las sentencias que tiene especificadas.

Este tipo de fraude presenta una serie de ventajas para el delincuente sobre el resto de formas de comisión del fraude en general. Primero, es un delito que puede reportar a su autor cuantiosas ganancias sin suponer para éste un grave riesgo para su integridad personal ni para la de terceros. Segundo, es un delito que no deja rastro ya que se actúa sobre los cálculos que efectúa el programa, no sobre los datos de entrada. Y tercero, los autores al ser normalmente personal técnico especializado en el área de informática saben ocultar las huellas de la conducta

[158] Entendemos, de una forma simplificada, por programa un conjunto ordenado lógicamente de sentencias, escritas en un lenguaje de programación, a través de las cuales se ejecutan órdenes de cálculo matemáticas o lógicas sobre los datos de entrada, produciendo así un resultado de salida. Una definición más clara y concisa es la propuesta por el Prof. DAVARA al definir el programa como el "conjunto de órdenes o instrucciones que, siguiendo una lógica determinada, guían o dirigen las actividades del sistema (ordenador)." *Actualidad Informática Aranzadi* nº3, abril de 1992. Pág.4.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

delictiva.

En un rápido acercamiento al modo de comisión de la conducta delictiva se puede afirmar que los cambios sobre el programa se realizan normalmente sobre el programa fuente[159], no sobre el programa objeto[160].

Los cambios introducidos sobre el programa fuente se ejecutarán cuando el programa se compile y el nuevo programa objeto falseado sustituya al anterior.

Ante este panorama es necesario arbitrar algún sistema de control y prevención de estas acciones. Sieber[161] defiende como los más adecuados los controles de acceso que eviten un acceso incontrolado a los programas, estos controles de acceso deben de afectar a los propios programadores de la entidad. En definitiva lo que debe imperar es una división de funciones de forma que cada miembro de la entidad o de la institución de que se trate, sepa cuáles son sus obligaciones y que no puede tener acceso a cualquier función del sistema si previamente no está autorizado para ello.

Para finalizar los controles sobre este tipo de manipulaciones deben centrar su atención en tres áreas: el área del personal al servicio de la entidad, el área del procedimiento y la verificación de los resultados intermedios del proceso.

---

[159] Entendemos por programa fuente, siguiendo al Prof. DAVARA, el "programa escrito en lenguaje fuente y que, por tanto, necesita ser traducido a lenguaje máquina para que el ordenador le pueda ejecutar". "Lenguaje fuente se puede identificar con lenguaje de programación siendo aquél en el que el programador escribe las órdenes o instrucciones que constituyen el programa. El lenguaje de programación es el conjunto de símbolos, palabras, vocablos u otros medios de representación del conocimiento por los que se describen, mediante un convenio preestablecido, las órdenes o instrucciones requeridas para que el ordenador pueda ejecutar las operaciones o actividades deseadas". *Actualidad Informática Aranzadi*. N°3, abril de 1992. Pág.4.

[160] "Programa objeto es el resultado de la traducción de un programa que se encuentra en lenguaje fuente a lenguaje de ordenador". DAVARA RODRIGUEZ, M.A. *Actualidad Informática Aranzadi*. N°3, abril de 1992. Pág.4.

[161] SIEBER, Ulrich. Op. Cit. Pág. 19.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3.2.4.3. Manipulaciones de consola (hardware)

Hasta ahora hemos hablado de manipulaciones de datos o bien de manipulaciones de programas, en cualquier caso se trata de elementos intangibles. Pero las manipulaciones también pueden llevarse a cabo sobre elementos físicos del sistema de ordenador. Estas manipulaciones alteran el correcto funcionamiento de un elemento del servicio mecánico de la instalación del proceso de datos.

Un ejemplo de este tipo de manipulaciones lo constituyen las alteraciones físicas en cajeros automáticos (ATMs). Aunque indudablemente la seguridad a nivel hardware en cajeros cuenta hoy en día con dispositivos de:

- alarma sísmica, alarma que detecta vibraciones que tienen por objeto manipular algún elemento del cajero como el dispensador de billetes o la ranura de captura de tarjeta.

- Alarma de humos. Detectan incendios en la caja fuerte evitando la pérdida de dinero, y suelen ir conectados a un sistema de autoextinción mediante gases.

- Alarma frente a golpes. Detectan golpes de una cierta intensidad en el cajero.

- Alarma de temperatura. Detectan subidas en la temperatura de la caja y protegen frente a ataques con lanza térmica.

Estos sistemas de seguridad física se completan con la seguridad en la propia ubicación del cajero, en recintos cerrados o totalmente visibles al público, anclage al suelo, medidas antivandalismo como monitor de doble cristal y táctil por rayos infrarrojos. Sin embargo estas medidas no son de extensión generalizada en todo tipo de cajeros, y de hecho la obturación del mecanismo de captura de tarjetas que retiene ésta y posteriormente es expulsada y recogida por el delincuente que

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

previamente ha obtenido el PIN de esa tarjeta, se ha convertido en un tipo de manipulación, no habitual, pero sí con suficientes ejemplos para que ya hayan llegado a conocimiento de nuestros Tribunales.

A continuación reproducimos, dado el interés práctico del supuesto descrito, una demanda civil de reclamación de cantidad en que supuestamente los hechos base del perjuicio patrimonial ocasionado son los descritos (una manipulación del hardware de un cajero automático). Ante la dificultad de descubrir al delincuente, la víctima (titular de la tarjeta y de la cuenta corriente asociada) se ve obligada a interponer una demanda de responsabilidad civil frente a la entidad financiera depositaria de sus fondos.

AL JUZGADO DE PRIMERA INSTANCIA DE MADRID QUE POR TURNO DE REPARTO CORRESPONDA

D/Dª. **.....**, mayor de edad, de estado ...., de profesión ....., vecino de ....., con domicilio en la calle ..... de ....., provisto del Documento Nacional de Identidad núm. ....., letra .., expedido en ...., en fecha ..... de 199., vigente, ante el Juzgado comparezco y como mejor en derecho proceda, DIGO:

Que bajo la dirección de la Letrada del Ilustre Colegio de Abogados de ....., Dª Juana María Domaica Maroto, colegiada núm. ....., con despacho en ....., formulo **DEMANDA DE JUICIO DE COGNICION** contra la Compañía Mercantil **.....** inscrita en el Registro Mercantil de ....., con domicilio social en ....., **en reclamación de la cantidad de ..... pesetas** de principal, más intereses y costas, demanda que apoyo en los siguientes hechos y fundamentos de derecho.

HECHOS

PRIMERO.- D/Dª. ..... ha sido titular de la cuenta corriente ordinaria con código ..... hasta el día ..... en que procedió a su cancelación.

Se acompaña como DOCUMENTO Nº 1 certificado de cancelación de la cuenta nº .....

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Se designan a los oportunos efectos probatorios los archivos y registros de la entidad demandada donde obrará copia del contrato de cuenta corriente que unía a ésta con el demandante y de su correspondiente cancelación.

SEGUNDO.- A la cuenta identificada en el hecho anterior se encontraba asociada una tarjeta de débito tipo .. con número ..... válida desde .... hasta el .....

Se designan a los oportunos efectos probatorios los archivos y registros de la entidad demandada donde obrará copia del contrato de uso de dicha tarjeta.

TERCERO.- El día ....., alrededor de las 21.30 horas, el/la demandante acudió al cajero automático de la red ... que la entidad ....., S.A., dispone en su sucursal urbana nº ..... sita en la C/ .....

El/la demandante tras introducir la tarjeta identificada en el hecho segundo de esta demanda, de la que era titular, en el cajero no pudo efectuar ninguna operación quedando, así mismo, la tarjeta capturada por éste. El/la demandante abandonó el lugar tras intentar repetidamente recuperar la tarjeta confiando quedaba convenientemente custodiada en el cajero que la había capturado.

CUARTO.- Transcurrido el día ....., el ..... el/la demandante acudió a la sucursal urbana nº ..... del ....., S.A. con el fin de recuperar la tarjeta capturada.

Sin embargo, allí se le informó, siendo así sorprendido en su buena fe, que su tarjeta no se encontraba entre las retenidas en los dos días anteriores por el cajero que, como certifica el director de la precitada sucursal, D....., estuvo inoperativo desde las 20,59 horas del día ..... hasta las primeras horas del día .....

Se acompaña como DOCUMENTO Nº 2 el certificado del director de la sucursal urbana nº ..... , S.A. al que se hace referencia en este hecho.

QUINTO.- El demandante ante la inquietud de comprobar que no se encontraba su tarjeta entre las retenidas en la sucursal del Banco ..... contacta de inmediato

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

telefónicamente, el mismo día, con la oficina principal del Banco ..... **anulando la tarjeta de débito .....** de su titularidad. En la misma conversación telefónica consulta el saldo de su cuenta nº ..... siendo informado por parte del Banco ..... que ya se habían producido disposiciones con su tarjeta por valor de cerca de ..... pesetas.

SEXTO.- El/la demandante aunque confiaba en que tras la anulación telefónica de la tarjeta, el día ....., quedaba ésta definitivamente inoperativa quiso en una prueba más de su actuar diligente denunciar por escrito los hechos. Así el día ..... el/la demandante procedió a denunciar los hechos por escrito ante la oficina principal del Banco ..... sobreabundando, de este modo, en la denuncia telefónica de anulación de su tarjeta que efectuó el día .....

Se aporta como DOCUMENTO Nº 3 copia sellada del escrito al que se hace referencia en este hecho.

SÉPTIMO.- Asimismo, el/la demandante adoptando todas las medidas a su alcance, y jurídicamente exigibles, en orden a dar cuenta de los hechos recogidos en esta demanda formuló denuncia ante la autoridad competente, en concreto, ante el Juzgado de Instrucción de Guardia nº ..... el día .....

Se aporta como DOCUMENTO Nº 4 copia sellada por el citado Juzgado de Guardia.

OCTAVO.- **Pese a que el día ..... el/la demandante telefónicamente anuló la tarjeta de su titularidad,** siendo informado de que se habían producido hasta ese momento disposiciones por valor de ..... pesetas, **se siguieron produciendo después de la anulación de la tarjeta disposiciones no autorizadas por el/la demandante hasta un total de ..... pesetas**.

NOVENO.- Así pues tras quedar capturada la tarjeta .... del demandante por el cajero del Banco ..... S.A., el día ....., se produjeron **nueve cargos, que la demandada atribuye al uso de la tarjeta ....., que no realizó el demandante pues ya no tenía dicha tarjeta en su poder**, estos cargos son los siguientes:

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Se acompaña como DOCUMENTO Nº 5 consulta de movimientos de fecha ..... en el que se reflejan las disposiciones con tarjeta .... no realizadas por el/la demandante.

DÉCIMO.- El/la demandante plantearon reclamación ante el Defensor del Cliente de la entidad demandada, escrito de reclamación solicitando la devolución de los cargos identificados *ut supra.*

Se acompaña como DOCUMENTO Nº 6 acuse de recibo por el Defensor del Cliente del escrito de reclamación referido en este hecho.

DÉCIMO PRIMERO.- El Defensor del Cliente emite resolución desestimatoria a las peticiones del ahora demandante.

Esta resolución veladamente califica como negligente la conducta de D./Doña ..... SIN PRUEBA ALGUNA arrogándose atribuciones que como parte interesada no le corresponden, ya que es únicamente un Tribunal de Justicia el que puede considerar si una determinada actuación es culposa o negligente.

Asimismo, el Defensor del Cliente da por supuestos una serie de hechos (expulsión de la tarjeta por el cajero, captura de la misma por un tercero) sobre los que no aporta prueba alguna y sobre los que, sin embargo, funda su resolución.

Se acompaña como DOCUMENTO Nº 7 la resolución del Defensor del Cliente al que se hace mención en este hecho.

DÉCIMO SEGUNDO.- El/la demandante en su tortuoso camino en el esclarecimiento y reconocimiento de su total ausencia de responsabilidad en los hechos expuestos en este escrito de demanda, solicitó (con fecha.....) al sistema ....., S.A. información concreta sobre los siguientes puntos:

1º. Si el cajero, identificado en el hecho tercero de esta demanda, presentó permanentemente en pantalla el mensaje de encontrarse inoperativo entre las 20,59 hs. del día ..... y las primeras horas del día .....

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

2º. Si dicho cajero, en atención a la avería que sufrió en las fechas mencionadas en el párrafo anterior, pudo o no capturar tarjetas de los usuarios de la red que se acercaron al mismo para utilizar sus servicios.

Se acompaña como DOCUMENTO Nº 8 copia de la solicitud de información dirigida al Sistema .....

DÉCIMO TERCERO.- La contestación a esta solicitud de información no pudo ser más desalentadora al no arrojar ninguna luz sobre los hechos y recoger exclusivamente la misma información ya suministrada por el Banco ..... y añadir (se reproduce textualmente) que la **inoperatividad del cajero** es la "**única circunstancia que en este asunto puede ser constatada de forma fehaciente**". Por tanto de aquí se desprende la **unilateralidad y arbitrariedad de la atribución de responsabilidad al demandante** en base a una supuesta pantalla de aviso de error que aparece en todo cajero inoperativo y a la imposibilidad de que éste capture tarjetas.

Se acompaña como DOCUMENTO Nº 9 escrito remitido por el Sistema ..., S.A. al que se hace referencia en este hecho.

DÉCIMO CUARTO.- Quede constancia, a los efectos de ilustrar al juzgador, que el/la demandante desde hace más de quince años ha sido titular de cuenta corriente y de tarjetas de débito y/o crédito emitidas por la entidad demandada sin haber tenido ningún incidente, controversia o contestación con ésta.

Acreditada, así mismo, la negativa de **Banco .....** a asumir la responsabilidad en los hechos expuestos en esta demanda y no habiendo procedido, pese a los requerimientos efectuados desde el mes de ....., a devolver al demandante los importes indebidamente cargados en la que fue cuenta de su titularidad por disposiciones efectuadas, según manifestaciones de la demandada, por D/Dª..... hechos que el demandante niega rotundamente es por lo que se ve obligado a interponer la presente demanda.

A estos hechos son de aplicación los siguientes,

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

FUNDAMENTOS DE DERECHO

I.- JURISDICCIÓN Y COMPETENCIA

La competencia objetiva y territorial corresponde al Juzgado de Primera Instancia (**artículo 85 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial**) del lugar en que deba cumplirse la obligación, y a falta de éste, el del lugar del contrato (**artículo 62.1° de la Ley de Enjuiciamiento Civil**) en ambos casos .....

II.- PROCEDIMIENTO

Por tratarse en esta demanda de una cuestión entre partes cuyo interés excede de 80.000 pesetas sin pasar de 800.000 pesetas, ha de decidirse en juicio de cognición, según dispone el artículo 486, inciso primero, de la Ley de Enjuiciamiento civil, competencia de los Juzgados de Primera Instancia (**artículo 26 del Decreto de 21 de noviembre de 1952 por el que se desarrolla la base décima de la Ley de 19 de julio de 1944 sobre normas procesales aplicables en la justicia municipal).**

III.- SOBRE EL FONDO

1)DE LA RELACIÓN CONTRACTUAL QUE UNIA A DEMANDANTE Y ENTIDAD DEMANDADA

Entre demandante y demandada existió una relación contractual que se concretó en la cuenta corriente n° ..... donde se produjeron los cargos no consentidos por el demandante objeto de reclamación en esta demanda.

El depósito bancario de dinero en cuenta corriente, es un contrato *sui generis* y complejo que, con independencia de las liquidaciones periódicas necesarias para la determinación del saldo exigible previa conformidad de las partes, OBLIGA AL DEUDOR A DEVOLVER DICHO SALDO. Esta obligación según señala la **Sentencia del Tribunal Supremo de 25 de julio de 1991** TIENE CARÁCTER CASI ABSOLUTO.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

*"La **obligación de conservación y devolución**, que tanto el Código de Comercio como el Código Civil imponen al depositario, tiene carácter casi absoluto, y sólo decae mediante una causa muy justificada de fuerza mayor o de caso fortuito, no previsible ni evitable. Ello lleva a exigir la responsabilidad de la entidad bancaria por los menoscabos, daños y perjuicios que el demandante haya sufrido por su negligencia".* **(T.S. Sentencia de 25 de julio de 1991)**.

El depósito en cuenta corriente bancaria se caracteriza principalmente, según la doctrina mercantil, por la obligación que asume el Banco de efectuar el servicio de caja, atendiendo las órdenes de pago que recibe, con cargo a las sumas depositadas por su cliente. Dentro de este servicio de caja se incluyen todos los cobros y pagos realizados por el banco como comisionista del titular de la cuenta corriente.

En consideración a lo hasta aquí expuesto y en orden a la calificación jurídica de la relación contractual que existió entre los ahora demandante y entidad demandada, resultan de aplicación los preceptos del **Código de Comercio** que regulan los **contratos mercantiles de depósito y comisión** en los **artículos 303 a 310** y **244 a 280** respectivamente. Especialmente señalamos los siguientes preceptos del Código de Comercio: Artículo 306, Artículo 256.

Queda así expuesto que entre el demandante y la entidad demandada existió una relación contractual. De esta relación deriva la acción personal del que fue cuentacorrientista en reclamación de cantidad por cargos, contra las sumas depositas por éste en su cuenta corriente, no efectuados y por tanto no autorizados por él, D/Dª..... ahora demandante.

Resultan así mismo de aplicación los preceptos del Código civil que regulan tanto los contratos en general (artículos 1.254 y siguientes) como el mandato (artículos 1.709 y siguientes) y el depósito (artículos 1.758 y siguientes).

Por tanto ahora corresponde analizar: 1º la actuación del demandante-depositante-comitente y 2º determinar las obligaciones como **comisionista-depositario** de la entidad **demandada** y su responsabilidad por su incumplimiento.

2)DE LA ACTUACIÓN DEL DEMANDANTE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Analicemos detalladamente la actuación del demandante el día ..... en que alrededor de las 21:30 horas decidió acudir a un cajero de la red .... para hacer uso de su tarjeta .. con nº..... y obtener numerario.

1º. El demandante se acercó al cajero de la red ... situado en la calle ..... de .... y no observando ninguna anomalía en dicho cajero introdujo su tarjeta en el lector destinado al efecto.

2º. El demandante tecleó, como es operativa habitual, su Número de Identificación Personal (NIP) asociado a la tarjeta. Al comprobar que el cajero no respondía como era normal en otras ocasiones el demandante pulsó repetidamente la tecla de cancelación no consiguiendo, sin embargo, la devolución de la tarjeta. ¿Cabe apreciar alguna negligencia en la conducta del demandante? A criterio de esta parte NO. Muy al contrario, el demandante hizo uso de un sistema sobre el que no tiene el control directo (la red de cajeros) y con estricto cumplimiento de las normas de uso de cajeros automáticos (ATMs) obtuvo el siguiente resultado:

a) no pudo disponer del numerario que necesitaba esa noche del .....,

b) quedó privado de la tarjeta ... con la que podría haber obtenido el numerario que necesitaba en otro cajero y,

c) más grave aún, más tarde comprueba que en la cuenta corriente nº ..... de su titularidad se han producido cargos por importe de ..... pesetas, entre los días ....., por uso de su tarjeta .... cuando esta tarjeta no ha estado en su poder desde las 21:30 horas del citado día .....

3º. El demandante notificó telefónicamente al Banco ....., (entidad emisora de la tarjeta) tan pronto como no le fue reintegrada ésta la anulación de la misma, confirmando por escrito el día ..... la denuncia de los hechos ante la entidad Banco .....

De acuerdo con el relato fáctico expuesto el comportamiento del demandante se sujeta a lo jurídicamente exigible como bien queda patente a la luz de lo dispuesto en el Anexo de la **Recomendación de la Comisión de las Comunidades**

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Europeas, de 17 de noviembre de 1988, relativa a los Sistemas de Pago y en particular a las relaciones entre titulares y emisores de tarjetas (88/590/CEE) punto 4.2.: "*... siempre y cuando el titular cumpla con las obligaciones que se le imponen con arreglo a la letra a, primer guión de la letra b y la letra c del número 1 del presente punto, y no actúe con grave negligencia ni fraudulentamente cuando utilice su instrumento de pago,* ***no será responsable, previa notificación del daño que resulte de tal uso***".

En este mismo sentido se pronuncia el **Código de Buena Conducta del Sector Bancario Europeo relativo a los Sistemas de Pago mediante tarjeta, de 14 de noviembre de 1990,** que constituye la respuesta de las Asociaciones Europeas del Sector de Crédito (AESC) -es decir, la Agrupación de Bancos Cooperativos de la CE, la Federación Bancaria de la CE y la Agrupación Europea de Cajas de Ahorro- a la Recomendación nº 88/590/CEE de 17 de noviembre antes citada.

Este Código de Buena Conducta, como expresamente se recoge en su introducción, será de aplicación dentro del marco legal de cada país.

El punto 3.6 apartado c) del Código de Buena Conducta impone a los titulares de las tarjetas la obligación de informar al emisor a la mayor brevedad la constatación:

"- *de la pérdida, el robo o la copia de la tarjeta o de los medios que permiten su utilización,*
- *del registro de operaciones no autorizadas sobre su cuenta,*
- *de cualquier error u otra irregularidad en el mantenimiento de la cuenta por el emisor*"

El punto 13 de este Código establece la responsabilidad del emisor de la tarjeta por el incorrecto funcionamiento del sistema de cajeros que él controla al decir:

"El emisor será responsable de las pérdidas directas en que haya incurrido el titular de la tarjeta derivadas de un incorrecto funcionamiento del sistema sobre el que el emisor tiene el control directo. *Los términos "pérdidas directas" se refieren únicamente al importe principal de la operación que se haya cargado en la cuenta del titular, incrementado por los intereses correspondientes.* ***El término "directo" se refiere a todos los aparatos y***

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

lugares en que el emisor ha autorizado la utilización de la tarjeta.

El emisor no será considerado responsable de las pérdidas derivadas de una avería técnica del sistema de pago si ella ha sido señalada al titular de la tarjeta mediante un mensaje en el aparato o de cualquier otra manera evidente".

La exoneración de responsabilidad del emisor en estos hechos no ha quedado acreditada pues el cajero que utilizó el demandante no presentaba señal alguna que indicara su inoperatividad. Y la inoperatividad en sí es la "**única circunstancia que en este asunto puede ser constatada de forma fehaciente**" como así reconoce el documento nº ... aportado junto a esta demanda.

Por último y de acuerdo con lo dispuesto en el artículo **1.104 del Código Civil**:

"...
Cuando la obligación no exprese la diligencia que ha de prestarse en su cumplimiento, se exigirá la que correspondería a un buen padre de familia".

El demandante desarrolló la diligencia exigible a su condición de cuentacorrientista custodiando la tarjeta de su titularidad hasta que ésta quedó capturada por el cajero y notificando su desaparición a la entidad emisora, demandada.

3)DE LOS INCUMPLIMIENTOS DE LA ENTIDAD DEMANDADA (Infracción de las normas del ordenamiento jurídico)

A) Infracción de sus obligaciones como depositario

De acuerdo con el artículo 306 del Código de Comercio transcrito *ut supra* la entidad demandada estaba obligada como depositaria del saldo de la cuenta corriente titularidad del demandante a conservar la cosa objeto del depósito y a devolverla cuando el depositante lo pidiera. Esta obligación fue incumplida por la demandada en tanto en cuanto permitió realizar unas disposiciones sin autorización del titular de la cuenta y tarjeta, demandante. Así pues dos son las actuaciones contrarias al tenor literal de sus obligaciones por la demandada:

1ª. No custodiar adecuadamente el instrumento de pago, tarjeta nº .....,

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

cuando ésta quedó capturada por el cajero de la red ... lugar donde el emisor de la tarjeta había expresamente autorizado su uso.

A estos efectos resulta altamente esclarecedora **la doctrina establecida por el Servicio de Reclamaciones del Banco de España,** entre otras, en la reclamación nº. 405/1989 donde expresamente declara que LA CUSTODIA DE LA TARJETA RETENIDA POR EL CAJERO ES RESPONSABILIDAD DE LA ENTIDAD. El Servicio de Reclamaciones del Banco de España considera que **la tarjeta encajada en un cajero queda bajo la custodia de la entidad siendo de su responsabilidad evitar que el instrumento de pago caiga en manos de un tercero**.

2ª. Los cargos enumerados en el hecho ..... de esta demanda responden a disposiciones en las que no se identificó al ordenante del pago ya que si se hubiera identificado, a dicho ordenante, no se hubieran producido.

En este sentido resulta de máximo interés la Sentencia de 20 de mayo de 1993 de la Audiencia Provincial de Ciudad Real (Sección 2ª) que en su fundamento de derecho cuarto dice textualmente:

"... lo cierto es que el usuario no se identifica ante el cajero automático, limitándose a digitalizar la clave numérica personal."

En este mismo sentido se pronuncia autorizada doctrina que reconoce: "... no cabe que el Banco compruebe la identidad de su cliente (otra cosa será cuando, como se prevé, los cajeros funcionen con huellas dactilares o la voz." (GOMEZ MENDOZA, M. *Naturaleza jurídica de las tarjetas de crédito, sus clases y carga de la prueba en el supuesto de extracciones en cajeros automáticos.*Revista de Derecho bancario y Bursátil año XIII Abril-junio 1994, página 494).

Como colofón y en orden a la determinación de las consecuencias de la falta de identificación del disponente, en los hechos objeto de esta *litis*, y la **fijación de la carga de la prueba** se destaca:

1º. La Sentencia de la Audiencia Provincial de Granada de 14 de diciembre de 1994 que en su fundamento de derecho primero declara: **"... era**

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

OBLIGACIÓN INDISPENSABLE la de identificar al titular, y este hecho corresponde acreditarlo a la entidad depositaria, al ser un HECHO EXTINTIVO de su responsabilidad, como exige el artículo 1214 del Código Civil.... con lo que aparece con nitidez la omisión de diligencia constitutiva de la CULPA CONTRACTUAL, y que obliga al demandado a indemnizar los daños y perjuicios causados, es decir las sumas reclamadas más sus intereses, de conformidad a lo que disponen los arts. 1100, 1101 y 1108 del Código Civil".

2º. La Recomendación de la Comisión de las Comunidades Europeas, de 17 de noviembre de 1988, relativa a los Sistemas de Pago y en particular a las relaciones entre titulares y emisores de tarjetas (88/590/CEE), que establece en su punto 6.1: "los emisores llevarán o procurarán que se lleven registros suficientemente detallados, de manera que quede constancia de las operaciones y puedan rectificarse los errores".

En el caso de los cargos no autorizados por el demandante **es el emisor el que tiene que probar que la operación fue correctamente registrada y contabilizada y no resultó afectada por alguna avería técnica o alguna otra anomalía** (punto 6.2 de la Recomendación 88/590/CEE).

B) Infracción de las NORMAS DE DEFENSA DE LOS CONSUMIDORES Y USUARIO

El **artículo 10 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios**, ampara al consumidor usuario de servicios bancarios. La Ley se aplica exclusivamente a aquellas relaciones en las que intervenga un consumidor en sentido estricto, es decir, consumidores finales de bienes o servicios. A efectos legales no ofrece problemas la equiparación entre la figura del consumidor y la del usuario, términos que deben considerarse análogos, si bien la figura del consumidor se relaciona más con los bienes y la de usuario con los servicios.

Centrado el ámbito subjetivo de aplicación de la Ley de Consumidores y Usuarios, siendo de aplicación a la presente demanda al quedar justificada la condición de usuario de servicios bancarios del demandante y siendo el otro polo de la relación una entidad de crédito subsumible en los términos de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

"empresas" y "grupo de empresas" que la ley utiliza, debe analizarse el artículo 10.1.c) 6°.

El **artículo 10.1.c) 6°** de la Ley de Consumidores y Usuarios declara **contrario al justo equilibrio de las contraprestaciones las limitaciones absolutas de responsabilidad frente al consumidor y usuario**, por tanto una liberación absoluta de responsabilidad del Banco ..... en las disposiciones enumeradas en el hecho noveno de este escrito de demanda infringiría lo dispuesto en el mencionado artículo 10.1.c) 6° y, por ende, el justo equilibrio de las contraprestaciones en la relación banco cliente.

Vuelve a ser en este punto altamente esclarecedora la Sentencia de la **Audiencia Provincial de Granada de 14 de diciembre de 1994** que en su fundamento de derecho tercero dice textualmente: "... la responsabilidad del demandado no nace del hecho del robo o hurto de la libreta de ahorros, pues este hecho por sí solo no hubiera desencadenado los efectos producidos si la referida entidad hubiera cumplido su anexa obligación de identificar al titular de la libreta, lo cierto es que dicha cláusula exoneratoria es inoperante, ya que tratándose de un contrato de adhesión el de autos, sus condiciones generales caen bajo la normativa de la Ley de Consumidores y Usuarios, de 19 de julio de 1984, al tratarse el actor de un consumidor final, y en concreto incurre en la nulidad prevista en el art. 10.4 de la citada Ley, en relación con lo establecido en el apartado 6 de la letra c) del número 1 de dicho precepto, que establece la exclusión de aquellas cláusulas que contengan limitaciones absolutas de responsabilidad frente al consumidor o usuario".

4) DE LA RESPONSABILIDAD CIVIL DE LA DEMANDADA BASADA EN SU INCUMPLIMIENTO CONTRACTUAL

Según los criterios de buena práctica bancaria sostenidos por el Servicio de Reclamaciones del **Banco de España** si el cliente de una entidad justifica un perjuicio real, como el que ha sufrido el demandante por importe de ..... pesetas, la entidad reclamada debe hacerse cargo del mismo, pues la **responsabilidad objetiva por fallos del sistema debe ser asumida por quien**

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

lo implanta, y no por quien lo utiliza, que además de no haber participado en la creación de dicho sistema, ve alteradas su confianza y expectativas de disposición.

El demandante como usuario de un servicio de expedición de efectivo a través de un cajero automático no tiene ninguna intervención en la puesta en funcionamiento del sistema, siendo un simple usuario del mismo. La imputación de las consecuencias dañosas de un incorrecto funcionamiento del sistema no le pueden ser atribuidas dada su falta de intervención en la puesta en funcionamiento de dicho sistema.

Se califica de fallo del sistema el hecho de que el cajero de la red ...., al que acudió el demandante a efectuar una operación el día ....., se encontrase inoperativo provocando la captura de su tarjeta y la posterior infracción de la obligación de custodia al permitir disposiciones sin el consentimiento del demandante.

Como ha quedado ya citado *ut supra* el número 3 apartado 13 del Código de Buena Conducta atribuye al EMISOR la RESPONSABILIDAD DE LAS PÉRDIDAS DIRECTAS EN QUE HAYA INCURRIDO EL TITULAR DE LA TARJETA DERIVADAS DE UN INCORRECTO FUNCIONAMIENTO DEL SISTEMA SOBRE EL QUE EL EMISOR TIENE EL CONTROL DIRECTO.

El término "pérdidas directas" se refiere al importe principal de la operación que en este caso asciende a ..... pesetas incrementado por los intereses correspondientes dice el Código. **En este caso y dado que no hay tipo de interés especialmente pactado en aplicación del artículo 1.108 del Código Civil se tomará el tipo de interés legal del dinero**.

Además, debe tenerse en cuenta que, en materia de cajeros, el **emisor responde frente al titular "por la no ejecución o ejecución incorrecta de las operaciones ... incluso cuando la operación se inicie a través de mecanismos electrónicos que no estén bajo el control directo o exclusivo del emisor"** (punto 7.1). Por tanto, la Recomendación atribuye responsabilidad al banco emisor de la tarjeta incluso cuando el cajero sea de otro banco, pero asociado al sistema ...

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

De la relación de hechos descrita en el cuerpo de esta demanda se deriva la clara actuación culposa del Banco ..... al no custodiar debidamente el saldo de la cuenta corriente del demandante, para lo cual se deben tener en cuenta los siguientes preceptos: **Artículos 1.101, 1.103, 1.104 y 1.106 del Código Civil.**

De esta forma, la indemnización que corresponde al demandante comprende no solo el importe que le fue cargado en su cuenta sin su autorización, sino también los intereses que se han generado y que se generen hasta que se dicte sentencia, y sin perjuicio de los intereses que legalmente corresponden durante la ejecución de la citada resolución.

IV.- INTERESES.

Incurren en mora los obligados a entregar o a hacer alguna cosa desde que el acreedor les exija judicial o extrajudicialmente el cumplimiento de su obligación, conforme al artículo 1.100 párrafo 1º del Código Civil, por lo que la demandada incurrió en mora respecto de la cantidad reclamada desde la fecha de la reclamación extrajudicial viniendo obligada al pago de los intereses legales desde aquel momento conforme a lo establecido en el artículo 1.108 del mismo cuerpo legal.

V.- COSTAS

Por aplicación de lo dispuesto en el artículo 523 de la Ley de Enjuiciamiento Civil corresponde la imposición de las mismas a la demandada.

Ejercitando cuantas acciones se deducen de lo expuesto

SUPLICO AL JUZGADO: Que presentado este escrito, con los documentos que se acompañan, se sirva admitir a trámite la **demanda de juicio de cognición contra** ..... y dictar sentencia ordenando:

I. Se condene a la demandada al pago al demandante de la cantidad de ..... **pesetas, más los intereses legales correspondientes desde la fecha en que la demandada incurrió en mora.**

II. **La condena a las costas derivadas del presente procedimiento a ..... entidad demandada.**

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

OTROSI DIGO: Que cumpliendo lo prevenido en el artículo 4º, último párrafo, de la Ley de Enjuiciamiento Civil, a fin de que se practiquen en él todas las diligencias que hayan de entenderse con el suscribiente, designo como domicilio en esta localidad el situado en la calle ....., por lo que,

SUPLICO AL JUZGADO: Se sirva tener por designado el mencionado domicilio.

OTROSI SEGUNDO DIGO: Que para mi defensa nombro a Dª Juana María Domaica Maroto, Abogado en ejercicio del Colegio de ....., que ha redactado esta demanda, y que, en prueba de aceptar también la dirección técnica de esta parte en el presente juicio, firma el presente escrito.

En su virtud,

SUPLICO AL JUZGADO: Se sirva tener por realizado el expresado nombramiento.

OTROSI TERCERO DIGO: Que teniendo la entidad demandada su domicilio social en la calle .....,

SUPLICO AL JUZGADO: Se dirija atento exhorto al Juzgado de igual clase decano de los de ..... con el fin de que se practique la notificación y emplazamiento de la demandada con traslado de la copia de la presente demanda.

Es Justicia que pido, en cuanto a principal y otrosíes, en .....

Firmado.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

3.3. El fenómeno INTERNET. Fraudes en la Red

Si hasta aquí hemos recogido la regulación penal del delito informático no podemos desaprovechar la ocasión para recoger un medio sobre el que muchas de las conductas descritas se están o pueden estar desarrollándose, nos referimos a Internet. El primer problema que nos encontramos es que en Internet no existe una regulación en relación a los usos abusivos que puede desarrollarse en ella.

En un reciente trabajo publicado por la Comisión de las Comunidades Europeas[162] se pone de manifiesto la gran potencialidad y, al mismo tiempo, la gran "miseria" de esta red de redes. Nos referimos al hecho de que Internet está conducida por los propios usuarios, y que son éstos, y no necesariamente editores establecidos, los que crean y suministran buena parte de los contenidos disponibles a través de la Red. Ésta funciona simultáneamente como medio de publicación y de comunicación, en definitiva, la red Internet difiere de los servicios tradicionales de telecomunicación y, precisamente, del adecuado tratamiento jurídico de esta diferencia depende el éxito de una posible futura regulación de Internet.

La Comisión de las Comunidades reconoce expresamente, en el documento que venimos comentando, la circulación de contenidos ilícitos y por tanto puede que incluso constitutivos de delito en algunos casos, en Internet. Ante esta situación la Comisión propone una serie de medidas para combatir las fuentes de las que proceden los contenidos delictivos. Como medida básica se configura la necesidad de incrementar la cooperación entre los Estados miembros en orden a intercambiar los datos de que se disponga en cada Estado sobre suministradores de contenidos ilícitos en la Red. Dada la falta de uniformidad entre las legislaciones de los Estados miembros en relación con qué se considera contenido ilícito en Internet se aconseja establecer unos criterios europeos mínimos.

---

[162] Comisión de las Comunidades Europeas. *"Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, sobre Contenidos ilícitos y nocivos en Internet"*. Bruselas 16 de octubre de 1996. COM (96) 487 final.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Asimismo, la Comisión propone fomentar la autorregulación[163] alentando el desarrollo de Códigos de Conducta en aquellos Estados miembros que todavía no dispongan de ellos. Pero, sin duda, entendemos que la solución ha de venir abordando la regulación de los ilícitos en Internet desde el punto de vista internacional, es decir, con la firma de un convenio internacional sobre contenidos ilícitos y nocivos.

Recogemos a continuación, brevemente, los posibles delitos que pueden desarrollarse sobre la red.

Delitos en INTERNET. Especial referencia a Fraudes Informáticos. Medidas de seguridad lógica en la Red

Como ya expusimos al comienzo de este trabajo un acercamiento al concepto de delitos informáticos, sean éstos cometidos dentro o fuera de una red como Internet[164],

---

[163] En el Reino Unido, Alemania, Países Bajos y Francia los suministradores de acceso a Internet ya han creado sistemas de autorregulación. En concreto en el Reino Unido se ha elaborado un Código de Conducta y se ha creado un organismo independiente denominado *Safety Net Foundation* que entre otras funciones presta servicios de valoración de grupos de debate y una línea directa para que el público denuncie los contenidos que el público considere ilícitos. En Francia se ha propuesto un Código de Conducta disponible en http://www.telecom.gouv.fr/english/sommaire.htm

[164] No es objeto de este trabajo el estudio del fenómeno Internet. Únicamente conviene hacer unas breves precisiones sobre el concepto que manejamos al referirnos a Internet. Primero decir que no es una red sino una red de redes. Es decir, Internet está formada por un inmenso conjunto de redes de ordenadores interconectados en todo el mundo. Salvo en algunos aspectos no está gobernada ni regulada por ningún organismo nacional o internacional.

Aunque Internet no tiene una arquitectura una organización de red definida, ya que crece y se desarrolla constantemente, sí cabe hablar de tres tipos de redes que configuran lo que es: las denominadas redes corporativas, las redes de operadores locales o proveedores de conexión y las redes de tránsito o proveedores de conexión internacional. Normalmente las entidades conectadas a Internet disponen de una red corporativa. A esa red están conectados una serie de puestos de trabajo que comparten la información de la corporación. La conexión a Internet de la red corporativa se realiza a través de los servicios de un proveedor de conexión. Un puesto de trabajo individual (un ordenador doméstico) puede acceder a Internet a través de los servicios de estos mismos proveedores. El proveedor de conexión garantiza la conectividad global, con cualquier punto de la red Internet. Esta conectividad la proporcionan las Redes de Tránsito que interconectan a nivel mundial las distintas redes de proveedores de conexión locales. Cfr. URIEL, Santiago. *"Internet. La red"*.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

exige una clasificación de estas conductas. Para ello nos inclinamos por un criterio simple como es la distinción entre **ataques activos** al sistema informático tanto a nivel lógico o de software (manipulación de datos y/o de programas) como a nivel físico o de hardware (destrucción y/o manipulación de elementos físicos del sistema); y los denominados **ataques pasivos** donde se accede de forma ilícita a la información que circula por la Red, o bien, a través de ésta a la información almacenada en un sistema[165].

Dentro de los que hemos denominado ataques pasivos las conductas más frecuentes son los accesos no autorizados. Según una corriente generalizada, tanto a nivel legislativo como doctrinal en todo el mundo, debe tipificarse como delito la entrada en un sistema informático sin la autorización del propietario. En estas conductas se produce un acceso inconsentido a un sistema sin alterar, inutilizar, destruir o de cualquier modo manipular los datos o los programas de ese sistema. El nuevo Código Penal español tipifica estas conductas en el artículo 197 pero desde la perspectiva de la defensa del bien jurídico intimidad. Esta podría constituir una crítica a la tipificación de las conductas delictivas relacionas con las tecnologías de la información y las comunicaciones en el Nuevo Código penal, en el sentido de que no se ha identificado un bien jurídico independiente objeto de protección, sino que se ha recurrido a bienes jurídicos tradicionales para identificar nuevas formas de ataque a ellos desde el ámbito de la informática y las comunicaciones.

Junto al acceso no autorizado a sistemas informáticos a través de la Red cabe otro tipo de ataques pasivos, igualmente tipificados por el nuevo Código Penal, como son la interceptación de mensajes de correo electrónico (e-mail).

Siguiendo con el criterio clasificador adoptado los ataques activos dentro o a través

---

"Tecnologías de la Información en la Empresa". Cuadernos de CINCO DIAS, nº 9. Madrid. 1996.

[165] Algunos autores, entre otros JAVIER RIBAS, entienden que aunque el delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando estas conductas delictivas se producen en el ciberespacio, en el mundo virtual de Internet, el concepto de delito informático se concreta en la agresión a los bienes jurídicos relacionados con las tecnologías de la información, es decir, datos, programas, documentos electrónicos, dinero electrónico, información. Cfr. RIBAS, Javier. *"Trascendencia Jurídica del Fenómeno Internet"*. Disponible en http://www.aui.es/congresos/p1.htm

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de la Red se concretan en: la destrucción de datos, las estafas electrónicas, las manipulaciones en transferencias de fondos, la infracción de derechos de autor y falsedades en documentos electrónicos.

De entre los ataques activos enumerados son las estafas electrónicas y las manipulaciones en transferencias[166] de fondos las que nos interesan como formas de fraude informático objeto de este trabajo.

Referencia a ataques reales producidos en la Red

Brevemente recogemos a continuación algunos ejemplos de los ataques más frecuentes y públicamente conocidos producidos en Internet.

Puede identificarse como uno de los factores que han propiciado y propician estas situaciones los propios protocolos de comunicación en Internet. Éstos se diseñaron para que fueran simples, careciendo de mecanismos de seguridad, siendo responsabilidad de cada usuario su implantación. Esta situación ha facilitado la proliferación de los denominados *sniffers* que acceden o escuchan los paquetes que viajan por la Red. En 1994 el 80% de los ataques en Internet se clasificaron en esta categoría. Los autores de estos ataques, denominados *crackers*, utilizan una serie de programas que les permiten escuchar los paquetes de datos que viajan por la red sin medidas de protección (un mensaje cifrado utilizando un sistema de encriptación asimétrico estaría a salvo de estos ataques). Así, por ejemplo, se averiguan passwords de cuentas bancarias para posteriormente acceder a ellas.

Junto a esta forma de violación de la información ha proliferado la suplantación de personalidad de usuario. Se denomina *hijacking* y consiste en tomar el control de una conexión ya establecida. El *hijacker* suplanta al usuario que realmente ha establecido la conexión dejándole colgado.

---

[166] Javier Ribas, a nuestro juicio, con un criterio acertado distingue entre estafas electrónicas donde cabe apreciar la existencia de un engaño a una persona (por ejemplo en una venta electrónica a través de Internet en la que el vendedor no suministra lo que publicita) y manipulaciones en transferencias de fondos donde el engaño es a un sistema informático. En cualquiera de los dos casos el tipo penal aplicable sería el de la estafa del artículo 248.2 del nuevo Código Penal. Cfr. RIBAS, J. *"Trascendencia Jurídica del Fenómeno Internet"*. Disponible en http://www.aui.es/congresos/p1.htm

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Ante las situaciones descritas se hace necesario adoptar medidas de seguridad que abarquen un doble ámbito el de la seguridad exterior o perimétrica, que impida a los usuarios situados en el exterior de un sistema acceder a su interior[167] si no se cumplen determinadas condiciones, y el de la seguridad interior o interna que impida a los usuarios interiores incumplir las normas establecidas. Cabría a nuestro juicio añadir las medidas de seguridad en la comunicación con el exterior. A ello dedicamos a continuación unas líneas en relación con las medidas de seguridad lógica en Internet.

Junto a los ataques activos y pasivos enumerados en los que el objeto de ataque es un bien o derecho relacionado con el tratamiento automático de la información, la red mundial Internet está sirviendo de campo de desarrollo de delitos tradicionalmente desarrollados en el mundo real en oposición al mundo virtual al que nos venimos refiriendo. En concreto hablamos de delitos de espionaje, terrorismo, narcotráfico, delitos contra la libertad sexual ...

Medidas de seguridad lógica en Internet. Trascendencia jurídica

Brevemente nos referiremos ahora a medidas de protección lógica frente a manipulaciones desautorizadas de mensajes que circulan por la red Internet y que pueden constituir una forma de comisión de fraude informático. El mensaje objeto de una manipulación desautorizada bien puede tratarse de una orden de transferencia de fondos o de pago con tarjeta. Entrarían por tanto estas conductas de lleno dentro del objeto de nuestro interés, manipulación intencionada (con ánimo de lucro) producida sobre o por medios informáticos y con repercusiones negativas en la esfera patrimonial de un individuo.

[167] En este ámbito de seguridad se situarían las redes *Firewall* (cortafuegos), a través de las que se protege una red segura de otra u otras no fiables. Las funciones básicas de un cortafuegos son: controlar todo el tráfico de entrada y salida de la organización, permitir únicamente el tráfico definido en la política de seguridad y el propio cortafuegos debe ser capaz de autoprotegerse frente a los ataques. El 80% de los cortafuegos consisten en *Router con filtering* que selectivamente permiten o deniegan el tráfico en el nivel de red. Cfr. GONZÁLEZ SÁNCHEZ, Jose Luís; SÁNCHEZ ALONSO, Mª Soledad. *"El problema de la seguridad en Internet"*. Mundo Internet 97. II Congreso Nacional de Usuarios de Internet e Infovía. Libro de Sesiones Prácticas. Madrid. Febrero 1997. Pág. 593 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En opinión de los expertos[168] los requerimientos de seguridad en redes abiertas como Internet se centran en proporcionar servicios de privacidad, integridad, autentificación y disponibilidad de la información. Así mismo aconsejan que estas medidas se seguridad se sitúen en los extremos o nodos finales de la red. Las manipulaciones de mensajes, alteración de información, dentro de la red Internet (ataques activos) no pueden ser prevenidos, sólo pueden ser detectados. En cualquier caso la criptografía se presenta como el principal mecanismo de seguridad en redes abiertas como Internet.

La adopción de estos mecanismos de seguridad responde en determinados casos a exigencias prácticas de evitación de incidentes y si los mensajes que circulan por la red tienen como fin la conclusión de acuerdos contractuales, aunque ciertamente en derecho español rige como principio general la libertad de forma[169], con el fin de evitar los siempre conflictivos problemas de prueba es recomendable adoptar sistema de encriptación que doten a los mensajes de los atributos de integridad, confidencialidad, autentificación y no repudio.

[168] FERNÁNDEZ GONZÁLEZ, José. *"Firma de Documentos Electrónicos: Firma Digital"*. Publicación interna P3K Sistemas de Información. Madrid. 1994.

[169] Artículo 1258 del Código civil: *"Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley"*.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

4. POSIBLES SISTEMAS DE CONTROL DEL FRAUDE INFORMATICO

4.1. CONTROLES A PRIORI

4.1.1. AUDITORÍA INFORMÁTICA

4.1.2. CONTROLES FÍSICOS. MEDIDAS TÉCNICAS DE PROTECCIÓN DEL HARDWARE

4.1.3. MEDIDAS DE SEGURIDAD PERSONALES

4.1.4. CONTROLES LÓGICOS

4.1.5. LA AMENAZA PENAL

4.1.6. CÓDIGOS ÉTICOS

4.1.7. PÓLIZA DE SEGURO PARA RIESGOS INFORMATICOS

4.1.8. ASIGNACIÓN DE UN PRESUPUESTO INTERNO PARA CUBRIR POSIBLES PERDIDAS ECONÓMICAS POR FRAUDE. (AUTOSEGURO)

4.2. MEDIDAS DE PROTECCIÓN A POSTERIORI

4.2.1. REPARACIÓN DEL DAÑO POR VÍA FINANCIERA

4.2.2. REPARACIÓN DEL DAÑO POR VÍA JUDICIAL

4.2.3. PLANES DE CONTINGENCIA. RECUPERACIÓN DE UN SISTEMA INFORMATICO ANTE UN EVENTUAL DESASTRE PROVENIENTE DE UNA ACTUACIÓN FRAUDULENTA

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

4. POSIBLES SISTEMAS DE CONTROL DEL FRAUDE INFORMATICO

Se pretende constatar en esta última parte de la investigación las posibles vías de control de los riesgos originados por las conductas constitutivas de fraude informático. El análisis, por tanto, se centrará en el estudio de la seguridad en un sistema informático genérico y, ante un posible ataque a esa seguridad, en los sistemas que tanto "a priori" como "a posteriori" pueden defender la integridad del sistema.

En primer lugar resulta de vital importancia desarrollar la seguridad de un sistema informático al mismo tiempo que éste se implementa. No es infrecuente desarrollar todo el sistema informático y después pensar en su seguridad. Esta situación normalmente provocará que la seguridad no se encuentre bien integrada en el sistema, que aparezca como un añadido de éste pero no formando una unidad con él. Esta situación puede venir provocada, como señala Méndez Cruz[170], por la consideración por parte de las empresas de la seguridad informática como gasto no como inversión. El primer paso antes de establecer un sistema de seguridad es hacer una valoración de los riesgos a los que se encuentra expuesto el sistema. Y aprender de los propios errores, es decir, hacer una planificación de la seguridad cíclica. Ante una violación de la seguridad del sistema se deben adoptar una serie de medidas básicas: examinar la forma en que el sistema en su conjunto ha sido afectado, analizar las causas del incidente rectificando los posibles puntos débiles del sistema que facilitaron la agresión, desarrollar un análisis de riesgos teniendo en cuenta el incidente y, una vez controlado el ataque al sistema, emprender las acciones legales pertinentes contra los presuntos autores de la agresión. Como ya se expuso con anterioridad, el riesgo de denunciar la agresión sin previamente controlarla es superior incluso al riesgo que ha producido el ataque. Un ataque no controlado hace totalmente vulnerable al sistema, por ello se vuelve a hacer hincapié en la necesidad de contar con un sistema de seguridad propio que permita reaccionar ante un ataque indicando dónde se encuentra el origen de la agresión y sus consecuencias. Un sistema de seguridad no sólo prevendrá agresiones sino que también ante una agresión ya producida debe proporcionar la información que permita determinar dónde y cómo se produjo la violación del sistema, al menos esto es lo deseable.

---

[170] MENDEZ CRUZ, Mario. *Falta cultura de seguridad informática en las esferas que concentran el poder de decisión en las organizaciones.* Seguridad Informática, N° 8, diciembre 1993. Año II. Pág. 33 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Haciendo un esfuerzo de síntesis se puede afirmar que la protección de un sistema informático, desde un punto de vista estrictamente fáctico, proviene de la limitación de las personas que tendrán acceso al sistema y en segundo lugar de las operaciones que les están autorizadas una vez dentro de dicho sistema[171]. El primer grupo de medidas se analizarán bajo el epígrafe: "Medidas de seguridad personal". Al análisis del segundo grupo se dedicará el punto de los controles lógicos.

En lo que se ha denominado medidas de seguridad personales su correcto desarrollo exigirá no sólo pedir la identificación de todo aquel que quiera acceder al sistema sino que demuestre que posee la identidad que alega. En definitiva se hace necesario un sistema de autentificación personal. Es muy importante destacar la necesidad de inculcar en toda empresa o institución que la tarea de la seguridad del sistema de información no es responsabilidad exclusiva del centro de proceso de datos sino que incumbe a todos los miembros de ese grupo de trabajo. Esta es la idea a la que hace referencia Méndez Cruz[172] con el nombre de "seguridad descentralizada". De acuerdo con esta teoría todos los empleados deben conocer los programas de seguridad y la trascendencia de su cumplimiento y los perjuicios que pueden derivarse de su incumplimiento. En definitiva lo que se considera un error es confiar la seguridad de un sistema informático a un conjunto reducido de personas dentro del grupo de trabajo, sin concienciar a éste en general de la importancia de mantener la seguridad de la información. Esta idea de la seguridad descentralizada lleva consigo una necesaria coordinación. Para Méndez Cruz es fundamental contar con la figura del responsable de seguridad que junto a funciones de control desarrolla otras de coordinación y divulgación de los programas de seguridad.

En armonía con lo expuesto hasta ahora Pérez Gómez concibe la seguridad informática en forma global y entiende que debe "abarcar tanto al ordenador como al sistema y a la red, lo que implica adoptar un plan de seguridad que se integre dentro de los objetivos generales de la organización"[173]. El logro de este sistema de seguridad informática en la

---

[171] En este sentido resulta de interés la opinión de Mario Méndez Cruz que señala como pilar básico sobre el que debe edificarse la seguridad de un sistema de información el principio general de "que cada miembro de la organización sólo acceda a los datos necesarios para realizar su trabajo". Cfr. MENDEZ CRUZ, M. *Falta cultura de seguridad informática en las esferas que concentran el poder de decisión en las organizaciones*. Seguridad Informática. N° 8. Diciembre 1993, Año II. Pág. 33 y ss.

[172] MENDEZ CRUZ, M. Op. Cit. Pág. 34.

[173] PEREZ GOMEZ, José Manuel. *La Organización Empresarial ante los Fraudes Informáticos*. ESIC-MARKET. 1988, 61. Julio - Septiembre. Pág. 91 y

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

empresa pasa por respetar u observar tres objetivos fundamentales: la continuidad de la explotación informática, la integridad de los datos y la confidencialidad de esos mismos datos y de los resultados de su tratamiento automatizado. Estos tres objetivos o estas tres premisas deben guiar todo tratamiento automatizado de la información dentro de la empresa o de la institución de que se trate. De acuerdo con esto los tratamientos de datos se deben desarrollar en la forma y plazos previstos, los datos que se procesan han de ser correctos, exactos y estar autorizada su manipulación informática. Por último, y en consonancia con el tercer objetivo, la información debe llegar únicamente a las personas que la organización haya previamente fijado.

No se debe finalizar esta pequeña sección de introducción sin pasar por alto el trabajo que la Unión Europea viene realizando sobre seguridad de los sistemas de información. No se debe olvidar que la universalización de la utilización de las nuevas tecnologías para el intercambio de datos, requiere contar con unos criterios comunes en materia de seguridad y la Unión Europea cuenta con los mecanismos normativos necesarios para conseguir esa convergencia.

El desarrollo de criterios de seguridad comunes en sistemas informáticos no sólo permitirá intensificar el número de transacciones entre países, sino que al mismo tiempo facilitará la persecución e investigación de todas aquellas conductas que de uno u otro modo hayan vulnerado los requerimientos de seguridad del sistema de información. La seguridad de los sistemas de información es objeto de estudio por el SOG-IS[174].

4.1. CONTROLES A PRIORI

En este punto queremos recoger un grupo de medidas de prevención que sirvan para proteger al sistema informático de la empresa de las agresiones al mismo. La primera de estas medidas, ya apuntada anteriormente es la separación física del sistema informático del resto de servicios y departamentos de la empresa. Esto implica necesariamente una división de funciones y la identificación con un código personal para cada empleado evitando así el acceso incontrolado desde cualquier terminal al sistema informático. En segundo lugar deben existir mecanismos regulares en todas las fases de operación del sistema, auditorías externas e internas,

ss.

[174] Senior Oficials Group of Information System Security. Grupo perteneciente a la Comisión de la Unión Europea.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

la concertación de pólizas de seguro y la asignación de unas cantidades por las empresas para la cobertura de las pérdidas esperadas por estas causas (autoseguro). Junto a estas medidas no debemos olvidar aquellas que juegan un papel disuasorio como es la amenaza penal y otras, como la existencia de unos códigos éticos[175], que ejercen una presión moral sobre el potencial delincuente.

Las medidas de prevención a que venimos haciendo referencia también reciben el nombre de medidas correctivas[176] y su finalidad es detectar posibles conductas fraudulentas y de este modo evitar que se produzcan. Hevia recoge una serie de medidas que facilitan esta labor preventiva[177] que en gran medida coinciden con las ya expuestas.

4.1.1. AUDITORÍA INFORMÁTICA

Ya hemos puesto de manifiesto cómo cada día tiene una mayor importancia para la gestión de las empresas tanto sus sistemas informáticos como la información que éstos manejan. La consecuencia lógica de estas afirmaciones es que se hace necesario que estos sistemas informáticos sean seguros. Uno de los medios para comprobar que existe el nivel de seguridad adecuado en un sistema es la auditoría informática, interna y externa. Recogiendo datos estadísticos de empresas españolas en el año 1989[178] el gasto medio anual en seguridad informática en España fue de 3,9% sobre los gastos totales de informática.

---

[175] Cfr, PARKER. *Fighting Computer Crime*. New York, 1983. Pág. 189 y ss.

[176] HEVIA, Eduardo. Op. Cit. Pág. 39 y ss.

[177] "- Diseño de informes que verifiquen la integridad, coherencia y consistencia de la información: interrelacionando ficheros, conformando, cuadrando cuentas y verificando cantidades totales. - Programas que calculen ratios y relaciones entre los valores críticos, alarmas por cuotas o topes establecidos. - Seguimiento diario del uso del ordenador, de los procesos ejecutados, de los recursos empleados, disponiendo de informes de ayuda que detecten las excepciones. - Existencia de pistas de auditoría sobre los datos principales, de manera que permanezca la huella de cualquier cambio o acceso sobre los mismos. - Verificación periódica de los datos, utilizando las pistas de auditoría y técnicas de muestreo verificativo. - Utilización de juegos de ensayo y procesos de simulación. - Disponer de un servicio de auditoría informática que verifique el correcto funcionamiento de los controles." HEVIA, E. Op. Cit. Pág. 39

[178] Informe de Price Waterhouse en colaboración con el Ministerio de Industria y Energia 1989. Tribuna Informática, 26 de febrero de 1991.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Algunas empresas gastaban más del 10% de su prepuesto para informática en seguridad y un 16% declararon no gastar nada en materia de seguridad. Entre las empresas que adoptaban medidas de seguridad un 28% de estas empresas respondió que era la auditoría informática el sistema de seguridad elegido.
La auditoría, desde una perspectiva general, se puede decir que se ocupa de revisar la seguridad tanto física como lógica de un sistema de información. Pero la auditoría puede tener un terreno mucho más amplio como es la comprobación de la eficiencia y la eficacia de las técnicas empresariales, comprobación del cumplimiento de políticas, de acuerdos entre empresas, de objetivos y planes, o de la normativa legal aplicable. Siguiendo a Miguel A. Ramos[179] podemos decir que la auditoría informática comprende "la revisión y la evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes de: 1º, el entorno informático de una entidad, abarcando todas o algunas de sus áreas, como: equipos, sistemas operativos, paquetes, aplicaciones y el proceso de su desarrollo, organización y funciones, las comunicaciones y la propia gestión de todos los recursos informáticos. 2º Las políticas, los estándares y procedimientos en vigor, su idoneidad así como el cumplimiento de: dichas políticas, estándares y procedimientos, los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y un análisis de los riesgos".

Vemos cómo la auditoría informática toca puntos vitales para conocer el grado de "inmunización" de un sistema frente a un fraude informático. Ámbitos como el control de equipos, comunicaciones, grado de satisfacción de usuarios y directivos son el origen, en multitud de ocasiones, de una acción fraudulenta.

El resultado de esta investigación se plasma en un informe escrito donde deben reflejarse los puntos de más alto riesgo dentro de la empresa auditada y, en el caso que nos ocupa, los fraudes detectados. Pero para llevar a cabo con total eficacia esta labor de control interno[180] estamos de acuerdo con Hevia y

[179] RAMOS, Miguel A. *Contribución a la mejora de las técnicas de auditoría informática mediante la aplicación de métodos y herramientas de ingeniería del conocimiento*. Septiembre 1990. U.P.M.

[180] "Se puede definir el control interno como el conjunto de medidas y procedimientos adoptados por la dirección de una entidad con el objeto de asegurar: la protección de sus activos (contra errores, irregularidades y otros riesgos); la fiabilidad de su sistema contable; la promoción de la eficiencia en las distintas áreas de la empresa; el cumplimiento de las

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Lafuente[181] en que el auditor necesita de una preparación especial para la detección de este tipo de conductas. Además un seguimiento adecuado exige la vigilancia del presunto defraudador más allá de su actividad exclusivamente laboral.

Una vez expuestas desde una perspectiva muy general las bases de la auditoría informática conviene establecer aquí la relación existente entre este sistema de control a priori del fraude informático y una de las medidas de protección a posteriori: los planes de contingencia. Es fundamental, en toda auditoría informática, establecer como base de la misma una serie de planes: un plan de protección de registros vitales, un plan de respaldo y recuperación, un plan de contingencia, e integrarlos todos a su vez en un plan de seguridad general. En relación con el plan de contingencia el auditor debe revisar que el plan se actualice y se pruebe periódicamente.

Haciendo un breve resumen de los objetivos que debe cubrir una auditoría informática[182] ésta debe revisar la seguridad de los siguientes elementos: la ubicación del centro de proceso de datos, la infraestructura del centro de proceso de datos, los equipos, el sistema operativo, los programas de seguridad con los accesos lógicos y contraseñas, los ordenadores personales y la informática de usuario final, las bases de datos en uso dentro de la empresa, las comunicaciones de datos tanto internas como el sistema de comunicaciones externas y como punto fundamental de revisión destaca el estudio de la implantación real de todo el sistema de seguridad en el quehacer diario del personal de la empresa.

Para finalizar, si ya hemos expuesto los puntos de mira donde debe fijar su atención el auditor informático, deben exponerse ahora las áreas de responsabilidad que tiene encomendadas. Primero es responsabilidad de la auditoría interna la disuasión del fraude mediante la evaluación de la adecuación y efectividad del control. Segundo es igualmente responsabilidad de la auditoría

---

políticas de la dirección". SNEYERS, A. Op. Cit. Pág. 155.

[181] HEVIA, E.; LAFUENTE, J.J. Op. Cit. Pág. 23 y ss.

[182] Si la auditoría es interna a continuación veremos los objetivos que debe lograr y si es externa debe revisar en qué medida la auditoría interna está cumpliendo con esos objetivos.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

la detección del fraude. En la función de detección el auditor debe prestar especial atención a las debilidades del sistema de control pues son estas debilidades los indicadores de que el fraude puede ya haberse cometido. La tercera responsabilidad del auditor recae sobre la investigación del propio fraude. No es tarea fácil pero sí de trascendental importancia preventiva descubrir las posibles complicidades existentes en una acción de fraude informático. La determinación del autor o autores es fundamental en el camino de la investigación, así como coordinar las acciones con el personal directivo y la asesoría jurídica. A la vista de los resultados de la investigación el auditor, en colaboración con el gabinete jurídico, aconsejará o no el inicio de las acciones legales pertinentes. Por último el auditor cuenta con la responsabilidad de elaborar un informe final con las conclusiones sobre la investigación y las medidas que hasta el momento se han adoptado en relación con la conducta fraudulenta.

En conclusión, la auditoría informática se perfila como uno de los métodos más eficaces para comprobar que el control interno de una entidad ha sido o no burlado, y caso de deficiencias en este sistema la auditoría las pondría al descubierto. Es en entornos con controles internos débiles o inexistentes donde el delito informático hace su aparición y es precisamente ahí donde la auditoría juega un papel trascendental de "chivato" de estas insuficiencias en seguridad.

4.1.2. CONTROLES FÍSICOS. MEDIDAS TÉCNICAS DE PROTECCIÓN DEL HARDWARE

En este punto intentamos dar unas breves nociones de la importancia de la seguridad del aspecto físico, en cuanto aspecto estático de los locales donde se encuentran instalados los sistemas informáticos y de las medidas de seguridad que sobre los propios elementos hardware cabe establecer.

La primera cuestión a plantearse sería determinar las características del edificio que albergue el centro de cálculo o el centro de proceso de datos de la institución. La respuesta a esta trascendental cuestión pasa por la definición de un edificio que tenga los servicios integrados, es decir, que se pueda desde una sala de control conocer el estado de funcionamiento de todo el sistema.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En el tema de la seguridad física de edificios se distingue entre los denominados edificios automatizados y los edificios inteligentes. Manuel de la Pascua[183] haciendo referencia al informe INFRA, elaborado por el Instituto Cerdá en Cataluña, entiende por edificio automatizado "aquel edificio en el que se gestiona el funcionamiento de sus instalaciones mediante un sistema que permite un control integrado y centralizado de las alarmas y de todos los servicios de seguridad". Sin embargo en un edificio inteligente además de contar con la automatización de los servicios del edificio tiene también automatizadas las funciones y las telecomunicaciones. La inteligencia de un edificio viene determinada por tres factores interrelacionados: primero un edificio inteligente debe ser un edificio flexible, segundo debe existir una integración de servicios y tercero debe contar con un diseño adecuado. La flexibilidad de un edificio viene determinada fundamentalmente por el hecho de que los servicios con los que cuenta el edificio sean susceptibles de adaptación a nuevas necesidades, por ejemplo una ampliación del centro de proceso de datos o una variación en la estructura de las telecomunicaciones en la empresa. En cuanto al factor de la integración de los servicios el edificio inteligente debe contar con la automatización del control, gestión y mantenimiento de los servicios básicos. La automatización afecta fundamentalmente al control de seguridad en la fase de sistema de alimentación, protección contra el sabotaje, disfuncionamiento de instalaciones, detectores de presencia, detectores de vibraciones, seguridad informática, detección de niveles de seguridad, circuito cerrado de televisión, etc. La automatización de todos estos servicios puede prestar una cobertura de seguridad vital para evitar un fraude informático. Pero junto a la automatización de los servicios se ha hablado de la automatización de las funciones. Para automatizar la función el informe INFRA señala que deben automatizarse las siguientes cuestiones: el acceso al servicio telefónico privado, posibilidad de trabajar con instalaciones de trabajo integradas, etc. En resumen un edificio inteligente es mucho más seguro que un edificio automatizado y por supuesto mucho más que un edificio convencional. Por tanto si se desea la mayor seguridad en los controles físicos de las instalaciones informáticas debe ser el edificio inteligente la opción más adecuada.

[183] DE LA PASCUA, Manuel. *Seguridad Física*. SECURMATICA. I Congreso Nacional de la Seguridad en Entornos Informáticos. 7/9 Marzo 1990. Edición de ponencias. Pág. 195 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Al comienzo de este punto se ha delimitado su contenido en una doble perspectiva: controles físicos del edificio que alberga el centro de proceso de datos y controles físicos sobre los propios datos que procesa el centro. En relación con esta segunda perspectiva los controles que se suelen aplicar para salvaguardar la integridad y confidencialidad de los datos se pueden clasificar en dos categorías fundamentales: controles físicos y controles lógicos. De los segundos hablaremos más adelante. Los controles físicos sobre los datos son aquellas trabas e impedimentos que restringen y protegen el acceso a los dispositivos, medios mecánicos, elementos hardware y comunicaciones. Los controles físicos los vamos a clasificar en dos categorías: controles físicos sobre la red remota de comunicaciones y controles físicos sobre la red interna. Entre los controles físicos sobre la red remota de comunicaciones se pueden citar los siguientes: protección o vigilancia de los centros de conexión, agrupación de líneas de cables que dificulten las posibilidades de localización no autorizada de transmisiones, trazado de la línea por lugares vigilados o de difícil acceso, instalación de detectores de accesos desautorizados a la línea de transmisión. En cuanto a los controles físicos aplicados a la red interna resumimos como los más característicos los siguientes: la instalación de llaves de seguridad para la apertura de terminales, lectoras de huellas digitales o de fondo de ojo para restringir el acceso únicamente a los usuarios autorizados[184], tarjetas magnéticas de identificación personal para restringir el acceso al centro de proceso de datos, normas sobre manejo, apertura y cierre de terminales de cumplimiento general y obligado.

Con todo esto lo que se pretende es establecer una barrera selectiva que impida el acceso físico al local y al terminal, inteligente o no, que permite la manipulación de los datos de la institución. Es fundamental para lograr este objetivo de protección concienciar a la alta dirección que los gastos en seguridad son en realidad altamente rentables.

[184] Deliberadamente no hacemos referencia a los conocidos *passwords* pues, de acuerdo con la doctrina consultada, se puede afirmar que ha sido un sistema de control de acceso muy extendido en los últimos veinte años pero que no ha funcionado de forma realmente efectiva. Cfr. CORUM, P.J. *Software de Seguridad*. SECURMATICA. I Congreso Nacional de la Seguridad en Entornos Informáticos. 7/9 marzo 1990. Pág. 75 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

4.1.3. MEDIDAS DE SEGURIDAD PERSONALES

Como consecuencia de la conciencia de la importancia de la protección y del análisis de las fuentes de peligro hecho en la fase de auditoría informática, aparece la necesidad de prestar especial atención a las medidas de seguridad personales.

La puesta en práctica de medidas de seguridad personales adecuadas se configura como una medida adicional para la prevención de los delitos informáticos en general y para la prevención del fraude en particular.

En la contratación o incorporación de un nuevo trabajador al centro de proceso de datos no sólo deben evaluarse los méritos técnicos del candidato, sino que debe prestarse especial atención a la información que pueda proporcionar su anterior empresario en relación con su modo de desenvolverse en el trabajo. Los antecedentes desfavorables sobre el comportamiento de ética profesional no suelen reflejarse en el informe del trabajador pero sin embargo sí pueden obtenerse en una entrevista personal con el anterior empresario .

Dentro de las medidas de seguridad personales otro aspecto a tener muy en cuenta es fomentar un ambiente de honradez general en el trabajo. Cuidar la buena relación entre todos los miembros de la empresa y evitar, en la medida de lo posible, que alguien se sienta injustamente infravalorado.

4.1.4. CONTROLES LÓGICOS

Los controles lógicos consisten, generalmente, en claves o códigos asignados a personas gracias a los cuales se pueden realizar determinadas operaciones. En cierto modo ya hemos hablado de ellos al referirnos a las medidas de control físico del acceso a datos. Pero aquí, en el punto de los controles lógicos, se pretende hacer hincapié en las características lógicas que debe reunir el programa de seguridad y no en los elementos físicos que rodean a dicho programa.

La existencia de controles lógicos implica la existencia, a su vez, de claves lógicas que tienen asignadas unas funciones y unas habilitaciones. Junto a esta capacidad de actuación, que se asigna a cada clave lógica, hay establecida una

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

correlativa responsabilidad. De forma que la extralimitación en la capacidad de actuación de una clave se traduzca automáticamente en una obligación de responder por ese exceso.

Los controles lógicos más frecuentes los vamos a exponer clasificados en cinco categorías: controles lógicos sobre la red remota de comunicaciones, controles lógicos de la red interna, controles lógicos de acceso a la aplicación, controles lógicos para acceso a programas de software básico y controles lógicos sobre los datos.

Los controles lógicos sobre la red remota de comunicaciones deben cubrir al menos los siguientes extremos: control o análisis de las contraseñas y códigos utilizados para el acceso al sistema de comunicación, control del terminal emisor, encriptación de la información, un sistema que deje constancia de los intentos fallidos de acceso al sistema, aplicación de técnicas que garanticen la integridad de la información que es transportada por la línea[185].

Los controles lógicos de la red interna deben reunir las siguientes características: control del terminal emisor, posibilidad de encriptación de la información, sistema de control de intentos de fraude y sistema de comprobación de contraseñas.

---

[185] Con estas medidas intentamos proteger a la información en uno de los tres estados en los que se puede encontrar, concretamente en el estado de transmisión. Con las medidas apuntadas lo que se pretende proteger es la privacidad, integridad y disponibilidad de la información. Las posibles violaciones a la seguridad de la red pueden venir de conocimientos desautorizados, de manipulaciones desautorizadas o bien de la destrucción desautorizada de información. Ya sabemos que los fraudes informáticos habitualmente se configuran como manipulaciones desautorizadas de información. Una vez identificados los ataques que puede sufrir la información en la etapa de transmisión el siguiente paso es determinar los mecanismos de defensa frente a esos ataques. Ya se han apuntado algunos de esos mecanismos pero de una manera sintética podemos hablar de tres fundamentales: la encriptación de la información, el establecimiento de controles de acceso y controles de identidad. Los expertos en el tema afirman que hoy y en el futuro inmediato la criptografía es el principal mecanismo de seguridad en redes. En un proceso de encriptación o de cifrado de información intervienen los siguientes elementos: la propia información a cifrar, el algoritmo de cifrado y la clave de cifrado. El texto encriptado es el resultado de transformar el texto en lenguaje natural a través del algoritmo de cifrado, con el control de la clave a texto cifrado. Cfr. FERNANDEZ GONZALEZ, José. SECURMATICA. III Congreso Nacional de la Seguridad en Entornos Informáticos. Madrid. 1992.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

En cuanto a los controles lógicos de acceso a la aplicación se puede afirmar que son los más importantes ya que todo defraudador debe salvarlos y de su infranqueabilidad depende en muchos casos la comisión o no del delito. Estos controles suelen funcionar con la existencia de una serie de claves asignándose a cada clave una serie de facultades determinadas. Dependiendo de la clave que se posea se podrá acceder a todas las opciones de una aplicación, a distintas aplicaciones etc. Cada clave debe reunir las siguientes características: determinación de las aplicaciones a las que se tiene acceso con dicha clave, especificación dentro de cada aplicación de las opciones o funciones a las que se puede acceder y dentro de cada opción las operaciones que se pueden realizar con dicha clave. La asignación de las claves con facultad de alteración de datos de importancia como por ejemplo retenciones por IRPF, altas y bajas en la Seguridad Social, etc, debe conferirse a personal de máxima confianza y reducir el número de claves y de personas autorizadas para utilizarlas al mínimo posible.

En cuanto a los controles lógicos para acceso a programas de software básico deben ser lo más férreos posibles de forma que eviten cualquier acceso incontrolado al sistema operativo.

Por último el control lógico sobre los datos tiende a determinar quién está autorizado para alterar en cualquier aspecto (cancelación, actualización) un dato existente en el sistema.

En este punto se han expuesto, a nuestro entender, las medidas de seguridad más importantes para preservar nuestra información de ataques incontrolados. Las medidas de seguridad lógica no por su falta de tangibilidad pierden realismo en la tarea de prevención del fraude informático.

4.1.5. LA AMENAZA PENAL

Con esta expresión se quiere hacer referencia a la existencia de un delito específico dentro del Código Penal o de la legislación penal especial que ejerza una función de disuasión frente a la comisión de estas conductas por la pena que llevaría aparejada la acción delictiva. Sin embargo los propios penalistas consideran, en general, que el desarrollo de medidas de seguridad en otros

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ámbitos junto con una información que sensibilice sobre la posibilidad de abuso es más efectivo que el incremento de la tutela penal. Sin embargo también existen tesis contrarias[186] que defienden la necesidad del aumento de los instrumentos jurídico-penales como medios de intimidación que persuadan al futuro delincuente a desistir de su inicial propósito criminal. Por otra parte el efecto preventivo de las regulaciones jurídicas no penales es limitado, nos referimos por ejemplo a la responsabilidad civil[187].

De acuerdo con ello es general la convicción en los países de nuestro entorno socio-cultural de que no cabe renunciar por completo al derecho penal como instrumento preventivo y represivo. La siguiente cuestión a plantearnos es determinar si el vigente derecho penal es suficiente o no para abarcar los abusos que se cometen en el ámbito de la delincuencia informática. A esta cuestión ya dedicamos los puntos primero y segundo de este trabajo por lo que nos remitimos a lo ya expuesto.

Por último recoger de nuevo aquí la opinión mayoritaria de la doctrina, de la legislación extranjera[188] y de organizaciones internacionales en el sentido de entender como insuficientes los tipos penales tradicionales para abarcar las nuevas formas de la criminalidad informática.

---

[186] THOME. Sesión de expertos en protección de datos, 6. DAFTA 27-29 de octubre de 1982. *Tagungsband, Referate und Ergebnisse*, 1883, Pág. 243 y ss.

[187] En relación con la respuesta extrapenal a la comisión de abusos relacionados con el tratamiento automatizado de datos merece especial atención el régimen de Infracciones y Sanciones establecido en el Título VII (artículos 42 a 48) de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE Núm. 262 de 31 de octubre de 1992. Téngase así mismo en cuenta el artículo 18 del Real Decreto núm. 1332/1994 de 20 de junio, que desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre.

[188] Austria (transcrito en JABUREK/SCHMÖLZER, *Computerkriminalität*, Wien, 1985); Suiza (transcrito por SCHIMD, *Zeitschrift für schweizerisches Recht*, 1985); Gran Bretaña (consideraciones de la Scottish Law Commission; Australia, Grecia, Hong Kong, Japón, número especial 846 de la revista *Jurist*, octubre de 1985).

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

4.1.6. CÓDIGOS ÉTICOS

Otra medida suplementaria de protección frente al fraude la constituyen los acuerdos de empresa, códigos éticos o también llamados códigos tipo en los que se establecen una serie de obligaciones o deberes que los empleados de una institución tienen para con ésta independientemente de sus deberes dimanantes de la relación laboral con la empresa[189]. Como señala el Prof. Davara[190] estos códigos tipo ayudan a mejor proteger a los ciudadanos y mejor defender sus derechos reconocidos en la ley. Por tanto se configuran estos códigos tipo o códigos de conducta o códigos deontológicos como medidas complementarias para la mejor aplicación e interpretación de la ley. En el caso de la criminalidad informática la falta de regulación legal de la materia hace aún más interesante si cabe el establecimiento de estas normas de conducta.

Estas normas cuentan con la ventaja de adaptarse a las características específicas de cada empresa en particular. Pero deben redactarse con sometimiento y respeto pleno de la legislación nacional y negociación con los sindicatos, si procede, para contar con validez jurídica.

En definitiva con estos códigos de conducta se intenta crear en la empresa un clima de bondad y honradez, lo que en el ámbito anglosajón se denomina la "moral *lidership*".

4.1.7. PÓLIZA DE SEGURO PARA RIESGOS INFORMÁTICOS

La concienciación creciente de las empresas (y no sólo del sector privado, sino también, del sector público) en relación con la consideración de la informática como un activo más ha determinado, en época reciente, la aparición de una

---

[189] La Comisión de las Comunidades Europeas ha puesto de manifiesto en el documento: *"Contenidos ilícitos y nocivos en Internet"*, COM(96) 487 final, la necesidad de fomentar la autorregulación en el seno de la comunidad de usuarios y prestadores de servicios en Internet. Los Códigos Éticos o Códigos de Conducta desarrollados por los propios implicados (usuarios o responsables) de un sistema de tratamiento automático y/o transmisión de información se revelan como un medio adecuado de autocontrol de dicho sistema.

[190] DAVARA RODRIGUEZ, Miguel Angel. *Derecho Informático*. Aranzadi. Pamplona. 1993. Pág. 94 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

nueva póliza de seguros para cubrir el riesgo de pérdidas que se puedan producir como consecuencia de alteraciones fraudulentas de los datos almacenados en el ordenador.

Este seguro se ha introducido recientemente 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, incluso algunas grandes compañías aseguradoras lo desconocen por completo, pero 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: introducción fraudulenta de datos al ordenador, o manipulación fraudulenta de los mismos, diseños o modificación fraudulenta de programas, daños malintencionados causados a la información registrada en tarjetas, discos, cintas, y cualquier otro soporte de información, tanto si estos medios de registro se encuentran dentro de la institución como fuera de ella, robo, desaparición de tarjetas, cintas , discos y cualquiera otros soportes de información en la propia empresa o cuando están siendo transportados, fraude en las telecomunicaciones de la empresa, es decir, en los mensajes teletransmitidos por el asegurado. Por último se añade la cobertura de responsabilidad civil derivada de pérdidas producidas por manipulación fraudulenta de mensajes transmitidos por el asegurado.

Otras pólizas estructuran el riesgo asegurado en los siguientes apartados: 1. Seguro de sistemas informáticos. 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 cómo quedan incluidas las formas de fraude más típicas cubriendo al asegurado prácticamente 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

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 seguridad no son las más adecuadas, la aseguradora exige que se adopten las medidas de prevención necesarias para reducir el riesgo de fraude al mínimo. La importancia de este estudio previo de la empresa asegurada es vital porque a partir de él se ofertarán o no determinadas coberturas[191].

De las pólizas de seguro analizadas el capital asegurado se basa en el cálculo de la pérdida máxima probable dimanante de un posible siniestro.

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

Las exclusiones de la póliza de fraude informático se extiende a los siguientes puntos:

- Pérdidas que resulten de cualquiera de los riesgos cubiertos por la Póliza Global de Bancos.
- Pérdidas causadas por un empleado identificable del asegurado o por una persona o personas en colusión con cualquier empleado del asegurado.
- Las pérdidas de un ingreso potencial (lucro cesante).
- Las pérdidas indirectas o consecuenciales de cualquier naturaleza, o los daños de cualquier tipo por los que se pueda considerar al asegurado legalmente responsable, a excepción de los daños directos compensatorios producidos por una pérdida cubierta por la póliza de fraude informático.
- La responsabilidad asumida mediante acuerdo por el asegurado, a menos que dicha responsabilidad se hubiese ligado al asegurado aún en ausencia de dicho acuerdo.
- Los gastos en que incurra el asegurado en el establecimiento de la existencia o la cuantía de la pérdida cubierta por la póliza de fraude informático. - Las pérdidas resultantes de una amenaza.
- Las pérdidas de datos electrónicos en el transcurso de su envío por correo cuando el transporte no se haya efectuado en vehículos blindados.

[191] En relación con estos estudios previos ver **ANEXO I** *Propuesta de Seguro contra Fraude Informático*. Willis Faber Reaseguros de España, S.A.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

■ Las pérdidas causadas por fuego.

- Las pérdidas causadas por fallo mecánico o de construcción de los elementos físicos del sistema informático.

- Las pérdidas resultantes de la adquisición de material informático con instrucciones fraudulentas (virus informáticos)[192].

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 para 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 que se puede aumentar la cartera del seguro de daños materiales incluyendo nuevas coberturas en un paquete amplio de daños materiales, software, criminalidad informática, etc.

Dado que todavía no se encuentra muy extendida como póliza independiente la de fraude informático resulta interesante constatar 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 infidelidad de empleados.

Habiéndose constatado en la realidad que son en la mayoría de las ocasiones los "insiders"[193], 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.

---

[192] Ver **ANEXO II.** *Póliza de Lloyd's contra Delitos Electrónicos y a través de Ordenador.*

[193] Cfr. *Seguro de Infidelidad y Fraude Informático.* ***World Policy Guide.*** Colección Seguros nº 10, marzo 1995. Ediciones Recoletos. Madrid.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

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 una 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.

En este tipo de pólizas de fidelidad de empleados se distinguen dos categorías fundamentales: las denominadas pólizas comerciales abiertas con límite global (PLG) y las pólizas de fidelidad comercial abiertas con límite acumulativo (PLA). La cobertura de la PLA es casi la misma que otorga la PLG, al abarcar los daños a todos los bienes propios y a aquellos que se encuentren en poder del asegurado. Pero en las pólizas PLA el importe de la indemnización que se haya pactado se toma como límite de responsabilidad para cada empleado por separado, en caso de que la acción fraudulenta se haya llevado a cabo en complicidad. Esto quiere decir que el asegurador deberá abonar el importe completo de la suma garantizada por cada "insider" autor o coautor del fraude. Por eso la PLA se denomina póliza de garantías acumulativas, mientras que la PLG es una póliza de garantía única o límite global.

La razón de exponer aquí estas precisiones teóricas no es otra que servir de base para argumentar que la PLA es quizá la forma de cobertura más segura, desde el punto de vista del asegurado, para cubrir el fraude informático. La PLA es una forma de cobertura más arriesgada, es decir potencialmente más costosa para el asegurador, que la PLG en el caso de que los empleados actúen en complicidad y el asegurado logre identificar a todos los culpables.

Hay, asimismo, que tener en cuenta que en la tipología de muchos fraudes informáticos se encuentra implicado únicamente un empleado desleal a la empresa, aunque tenga cómplices fuera de dicha empresa, siendo por ello más aconsejable la cobertura PLA. Pero, en cualquier caso, debe hacerse una precisión o límite de colusión, es decir, un límite de indemnización máxima del asegurador en el caso de un fraude causado por varios empleados.

En conclusión, del análisis de las pólizas contra fraude por ordenador ofertadas en el mercado español se deduce el hecho de que estas pólizas, como ya antes ha

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

quedado apuntado, están diseñadas para ser pólizas acompañantes de la póliza global de bancos. La finalidad de la póliza contra fraude informático es proporcionar una cobertura contra los delitos relacionados con la informática que no estén cubiertos por la póliza global de bancos[194].

Vemos cómo, de momento, el seguro de fraude informático parece dirigido, o estar pensado, para entidades financieras, bancos y cajas en concreto, aunque la exposición al riesgo de fraude informático no es en absoluto exclusiva de estas entidades.

4.1.8. ASIGNACIÓN DE UN PRESUPUESTO INTERNO PARA CUBRIR POSIBLES PÉRDIDAS ECONÓMICAS POR FRAUDE (AUTOSEGURO)

Con el autoseguro se produce una retención[195] del riesgo dentro de la propia empresa. Cabe preguntarse si en el caso del riesgo de fraude informático es aconsejable su retención. Para contestar a esta pregunta debemos referirnos a la razón que anima a una empresa para retener este riesgo. Como en otr- decisiones de retención del riesgo la razón fundamental para la toma de e decisión es la mejora en el coste de la cobertura que supone inclinarse por la solución del autoseguro. La idea de la mejora en el coste puede venir determinada por distintas razones. La estimación de que la prima requerida por el asegurador es muy alta puede influir en la decisión de retener el riesgo. En el caso del riesgo de fraude informático, ésta puede ser una causa para acudir al autoseguro aunque también pueden citarse otras como las siguientes: las medidas de prevención de riesgos requeridas por el asegurador son consideradas excesivas, o es un riesgo no asegurable. El fraude informático sí es un riesgo

[194] Si algún suscriptor de la póliza de fraude por ordenador es también suscriptor de la póliza global de bancos, caso frecuente, como no es intención incrementar o duplicar la cobertura al asegurado, normalmente, se acuerda que la póliza de fraude informático (fraude por ordenador) no se considerará como cobertura de excedente ni como coaseguro.

[195] Con el término retención hacemos referencia al uso de fondos propios de la empresa para cubrir pérdidas accidentales. La retención, por tanto, es un conjunto de medidas financieras que tienden directa o indirectamente a compensar las pérdidas de un riesgo previsible.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

asegurable pero actualmente en el mercado asegurador español una empresa puede encontrarse con demasiadas "trabas" que la desaniman a asegurar el riesgo.

No es infrecuente encontrarnos actualmente con muchas empresas que llevan a cabo lo que se podría denominar una retención pasiva del riesgo de fraude informático. Con la expresión retención pasiva nos referimos al desconocimiento de la existencia de un riesgo y la asunción inconsciente de ese riesgo. La retención pasiva también se produce al infravalorar las consecuencias de un siniestro producido por una acción de fraude informático. Y por último cabría, así mismo, incluir dentro de la retención pasiva algunas actitudes irresponsables que ignoran las consecuencias de la criminalidad informática. Si estas fórmulas de retención pasiva se repiten sistemáticamente, sin duda, se pone en peligro la estabilidad de la empresa.

No obstante, junto a esta forma de la retención pasiva también es frecuente la denominada retención activa que supone un conocimiento y evaluación de los riesgos cuya cobertura se retiene.

Esta medida más que preventiva del fraude es una medida que a diferencia del seguro no traslada fuera de la empresa las consecuencias económicas perjudiciales de una acción de fraude informático. Es dentro de la propia empresa que puede sufrir la acción fraudulenta, donde se reserva una cantidad para cubrir las posibles pérdidas. El cálculo de esta cantidad presupone la existencia de estudios previos sobre los bienes que deben o quieren protegerse, sobre los riesgos a los que están expuestos estos bienes, en definitiva, sobre el alcance económico de la pérdida de estos bienes.

Por tanto en una retención activa del fraude se puede producir bien como una asunción planificada, donde se establecen mecanismos de financiación del riesgo para el caso de siniestro, o bien como una simple asunción donde no se establece ningún mecanismo de financiación especial. Al hablar de la financiación de la retención se puede hacer referencia a diversas formas de financiación. Una es tratar la pérdida como un gasto corriente del período cargándose en la cuenta de resultados. Esta forma de financiación, como gastos corrientes, no es aconsejable para el riesgo de fraude informático ya que suele ser únicamente adecuada para riesgos de frecuencia media-baja y, sobre todo, de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

baja intensidad. Otra forma de financiación es la provisión contable. Consiste en separar una parte del beneficio de la empresa equivalente al valor previsible de la siniestralidad del período por causa de fraude informático. Esta medida cuenta con la desventaja de que no se dote realmente una provisión para cubrir el riesgo informático o se dote insuficientemente, minusvalorando los riesgos, y ante un eventual fraude informático la empresa se encuentre totalmente desamparada. Otro problema que plantea este método de la provisión contable es que ésta ha de estar constituida en activos líquidos y con frecuencia estos fondos finalmente son requeridos por la dirección para cubrir otras pérdidas distintas a las previstas de fraude.

Existen otras formas de financiación de la retención como son la dotación de un fondo interno o un fondo externo o bien la concertación de una línea de crédito. La dotación de un fondo interno se forma con las aportaciones de cada unidad operativa de la empresa según la cota de riesgo a la que se encuentra expuesta. En la dotación de un fondo externo se paga a una entidad aseguradora unas aportaciones que son acumuladas y administradas por ésta.

En cuanto a la concertación de una línea de crédito ésta se puede estipular bien después del siniestro o bien antes del siniestro. En las líneas de crédito post-siniestro la fuente de financiación proviene de un banco que se compromete a prestar una cantidad cierta. No es una forma de financiación aconsejable si las pérdidas son muy elevadas. En la forma de financiación de línea de crédito pre-siniestro, éste se negocia antes de que ocurra la pérdida y la gestión de riesgos tiene más facilidad de planificar.

Existen otras formas de financiación como son la creación de empresas cautivas[196] que aparecen en las grandes empresas como consecuencia de la planificación de los riesgos en éstas.

[196] Una empresa cautiva es una compañía de seguros o de reaseguros participada al 100% por una gran empresa matriz. La única función de la empresa cautiva es el seguro o reaseguro de algunos de los riesgos de su empresa matriz o de sus filiales.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Para finalizar hemos de decir que las técnicas de financiación de la retención del riesgo de fraude informático pueden clasificarse como sigue: técnica del autoseguro, técnica del coaseguro, franquicias y deducibles, límites de indemnización, selección negativa de riesgos y seguro de valor real. Es únicamente en la técnica del autoseguro donde se produce la retención total del riesgo de fraude informático por alguno de los métodos ya descritos.

4.2. MEDIDAS DE PROTECCIÓN A POSTERIORI

4.2.1. REPARACIÓN DEL DAÑO POR VÍA FINANCIERA

En este punto nos remitimos a lo expuesto en el epígrafe 4.1.7. relativo al estudio de las pólizas de seguro al ser este el medio que hoy se utiliza con mayor frecuencia para la reparación del daño producido por el fraude informático.

No obstante conviene aquí hacer referencia a una nueva forma de contratos informáticos que por la vía de la reparación financiera pretenden mantener la actividad empresarial en el caso de que circunstancias previstas pero inevitables (podrían 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[197]. Se trata de una medida de aseguramiento que en algunos casos se configura como un contrato de seguro.

[197] 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. Madrid. 1994. Pendiente de publicación.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

4.2.2. REPARACIÓN DEL DAÑO POR VÍA JUDICIAL

Realmente las autoridades encargadas de la averiguación y las autoridades judiciales están lejos de ofrecer una solución real y eficaz al problema de la delincuencia informática.

La concienciación sobre el problema real que hoy supone la criminalidad informática todavía no ha calado en la judicatura. Aunque como hemos visto en las Sentencias de nuestro Tribunal Supremo ya empiezan a criminalizarse conductas que hace pocos años por desconocidas eran totalmente impunes.

El adecuado tratamiento judicial de estos delitos debe venir por una especialización del órgano judicial encargado de conocer de estas conductas. En Suiza y en Alemania ya se sigue este sistema. En Zurich existen autoridades competentes especializadas en la persecución de la delincuencia económica y dentro de este tipo de delincuencia se enmarca la criminalidad informática. Por otra parte en la mayoría de las oficinas criminales alemanas existen departamentos especiales que cuentan con personal especializado para el esclarecimiento de los hechos en un delito

informático. La colaboración estrecha entre policía, como personal investigador, y jueces, como autoridad encargada de establecer la respuesta jurídica a los hechos probados, es fundamental en estos delitos.

La especialización en jueces y policía es tan importante como el adecuado tratamiento por la legislación penal de estos temas y la adopción de medidas de seguridad por las empresas.

4.2.3. PLANES DE CONTINGENCIA. RECUPERACIÓN DE UN SISTEMA INFORMÁTICO ANTE UN EVENTUAL DESASTRE PROVENIENTE DE UNA ACTUACIÓN FRAUDULENTA

Si un centro de proceso de datos se ve afectado por una acción de fraude informático de gran magnitud nos encontramos con que las pérdidas financieras pueden llegar a ser elevadísimas. En el mejor de los casos estas pérdidas estarán cubiertas por una póliza de seguros, pero la verdad es que las pólizas de seguros no se revisan con la misma periodicidad con la que

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

cambian los componentes del equipo informático de la empresa. No se incorpora a la cobertura de la póliza la pérdida o daño de esos nuevos componentes o procedimientos informáticos y de este modo las pólizas puede que vayan quedando obsoletas. De forma que llegue una ocasión en que la producción de una acción de fraude de importancia haga prácticamente desaparecer la empresa y la indemnización de la compañía aseguradora se entregue ya a una empresa inexistente. Esta situación es la que precisamente debe intentar evitarse con el desarrollo de un adecuado plan de contingencia.

Así pues una vez que hemos fundamentado la necesidad de protección del centro de proceso de datos, para garantizar la continuidad de su servicio y por tanto la continuidad del negocio, es necesario desarrollar un plan de contingencia.

Un plan de contingencia puede definirse, siguiendo a Soler de Arespacochaga[198], como "el conjunto de procedimientos de tipo preventivo, cuya misión es aportar la infraestructura necesaria para la puesta en marcha de una recuperación del sistema, en caso de producirse un desastre".

En la definición de todo plan de contingencia deben establecerse una serie de fases que en su desarrollo sucesivo permitan, primero, la continuidad de la actividad de la empresa y, segundo, la recuperación de la empresa del desastre sufrido.

El establecimiento del plan debe comenzar por la definición de los bienes a proteger, la determinación de las amenazas que existen sobre esos bienes y la medición del grado de probabilidad de que ocurra un daño. Una vez con estos planteamientos debe analizarse con qué medios contamos para minimizar los riesgos. En este momento es cuando, como expone Gaspar Martínez[199], debe producirse una decisión de tipo económico para adecuar el coste de los medios empleados al riesgo de que ocurran los daños que se

[198] SOLER DE ARESPACOCHAGA, J.A. *La Seguridad Informática. Planes de Contingencia*. Gerencia de Riesgos.

[199] GASPAR MARTÍNEZ, Juan. *Plan de Contingencia: una necesidad cada día más imprescindible*. Dirección y Progreso. nº 107. Septiembre-octubre 1989. Pág. 60 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

tratan de evitar. Es la relación entre el nivel de seguridad adoptado y el nivel de seguridad óptimo el que dará el índice de seguridad del plan de contingencia.

El plan de contingencia debe estar constituido por "un conjunto de medidas interrelacionadas que conduzcan al restablecimiento de las actividades normales de la empresa en el supuesto de que algún suceso provoque la interrupción de estas actividades"[200]. En nuestro caso este suceso puede ser una acción de fraude informático. Un plan de contingencia es un proyecto muy complejo que cuenta con varias fases. Para Soler de Arespacochaga las etapas que deben contemplarse en un plan de contingencia son las siguientes: gestión de riesgos (análisis de riesgos, medidas a aplicar y financiación de los riesgos), sistemas de protección física, sistemas de protección lógica y diseño de un sistema de recuperación. Estudios recientes[201] parecen indicar que aunque el aumento anual de las cifras de fraude informático son del 10% el número de casos ha descendido, pero la pérdida por caso se ha multiplicado por diez. Por tanto la necesidad de adoptar planes que atiendan las consecuencias de estos desastres está sobradamente justificada.

A continuación se expone de forma muy sincrética la posible estructura de desarrollo de un plan de contingencia. En una primera fase se presta atención a los aspectos básicos que garantizarán el éxito futuro del plan. En esta primera fase se procederá a la formación del equipo que planifique la recuperación después del desastre y se deberá contar con la aprobación por parte de la alta dirección. Tras esta primera fase de preparación, la segunda tiende a determinar cuáles son las aplicaciones informáticas más importantes que deben recuperarse en el menor tiempo posible para garantizar la supervivencia de la empresa. En la tercera fase se deben definir los requisitos mínimos de "back up" para las aplicaciones que en la fase anterior se han determinado como fundamentales para garantizar la continuidad en el funcionamiento de la empresa. En esta tercera fase se determinará, asimismo,

[200] GASPAR MARTÍNEZ, J. Op. cit. Pág. 63.

[201] ACUÑA TORRES, J.M. *Planes de Contingencia*. SECURMATICA. I Congreso Nacional de la Seguridad en Entornos Informáticos. Marzo 1990. Edición de ponencias. Pág. 39 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

el lugar físico donde deben almacenarse las copias de seguridad. La cuarta fase tiende a establecer el procedimiento más rápido para recuperar las aplicaciones vitales para el funcionamiento de la empresa en caso de que el sistema de "back up" no cumpla con el objetivo previsto. En la quinta fase de un plan de contingencia, teniendo en cuenta los equipos ya definidos para la gestión de la recuperación, se establecen equipos adicionales con sus funciones específicas y las personas que los gestionan. Las fases que a continuación se desarrollan intentan precisar lo más posible los tipos de desastres que puede sufrir la empresa, y deben por tanto aquí determinarse las modalidades de fraudes o manipulaciones informáticas a las que puede verse sometida la empresa.

Como hemos indicado antes un elemento básico del plan de contingencia es la planificación de un sistema de recuperación. Lo más importante en un plan de recuperación es que sea efectivo y para ello ha de estar suficientemente entrenado y probado. El sistema de recuperación precisa de la existencia de unos equipos de recuperación. Esto supone, en la mayoría de los casos, contar con un centro de proceso de datos alternativo. Para que funcione este centro de proceso de datos alternativo es necesario contar con: un procedimiento alternativo de trabajo debidamente documentado, con equipos de proceso alternativos y con guías de actuación. Si se ha asumido por la empresa como estrategia de respaldo frente a un desastre informático, la existencia de un centro alternativo, éste puede ser un centro propio o bien un centro compartido.

En conclusión, y para terminar, el plan de contingencia es como un nuevo ser vivo que desde el momento que ve la luz necesita de constantes atenciones y cuidados. Una vez que se ha desarrollado un plan específico para una empresa se inicia un camino de trabajo constante para actualizar dicho plan a las nuevas necesidades de la empresa. No es una solución puntual y su mantenimiento requerirá una función dedicada específicamente a ello. El coste del mantenimiento periódico del plan queda sobradamente justificado con que en una única ocasión consiga mantener a flote la empresa después del vil ataque de un fraude informático.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

5. CONCLUSIONES

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

1º Debe valorarse de forma muy positiva la nueva tipificación, en el artículo 248.2 del Código Penal, del delito de estafa cometida por medio de alguna manipulación informática o artificio semejante. Esta valoración positiva se basa en el hecho del reconocimiento claro y explícito por el legislador de la trascendencia penal de las conductas de fraude informático. Dada la peculiaridad de estas conductas entendemos que el tipo de la estafa en su modalidad agravada (art. 250.1.7°) será el adecuado para abarcar todo el desvalor de estas conductas. En las acciones de fraude informático normalmente 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. Ciertamente este mayor desvalor puede verse castigado con la agravación de la pena que prevé el artículo 250.1.7° del nuevo Código Penal, al establecer que la pena del delito de estafa puede llegar hasta prisión de seis años y multa de hasta doce meses, si el delito se comete con abuso de las relaciones personales existentes entre víctima y defraudador o aprovechando éste su credibilidad empresarial o profesional.

No obstante esta valoración positiva, la elección por el legislador del tipo de la estafa para incriminar las conductas de fraude informático presenta un importante escollo jurídico. Si el engaño es elemento fundamental, columna vertebral de la estafa es realmente difícil aceptar que se pueda engañar a una máquina, a un proceso o a un sistema informático. Esta tesis es la que debían sostener los partidarios de la aplicación del tipo de la estafa a los fraudes informáticos antes de la tipificación actual. Se planteaba así una línea de argumentación cuanto menos paradójica dado que una máquina no tiene conciencia ni voluntad. La situación se ha salvado, ciertamente con gran ingenio, por el legislador al tipificar como estafa la "manipulación informática o artificio semejante". Sin embargo, creemos que permanece latente la inadecuación del tipo de estafa para penalizar estas conductas.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

2º Si la respuesta penal que hoy cabe dar con el Código Penal español en la mano no nos satisface completamente ¿qué solución debe arbitrarse?. A nuestro entender ha de adoptarse una postura audaz. La solución vendría no tanto por la tipificación, como así se ha hecho en el art. 248.2 del CP de un nuevo delito de estafa informática, sino por el reconocimiento de un nuevo bien jurídico protegido: EL PROCESAMIENTO AUTOMÁTICO DE LA INFORMACIÓN. La protección del procesamiento automático (electrónico) de la información frente a los actuales ataques a los que se ve sometido permitiría establecer tipos penales específicos y propios de un bien de nuestro tiempo: la información tratada automáticamente.

3º En cualquier caso existe ya una creciente concienciación, tanto en el sector público como en el privado, sobre la necesidad de cubrir el riesgo de manipulación fraudulenta de los sistemas de tratamiento automático de la información. Se han intentado exponer en el último capítulo del trabajo los sistemas de defensa a los que se puede y se debe acudir. Consideramos que ante un incidente en un sistema informático (producido por una manipulación fraudulenta de éste) la conclusión a la que normalmente se llega es que "lo mejor es que nunca hubiera ocurrido", es por ello por lo que consideramos los sistemas preventivos, es decir, las medidas de seguridad lógica y física como las más adecuadas medidas de protección. Sin embargo las medidas de seguridad jurídica, (el recurso al sector asegurador, la reparación en vía judicial dada la nueva tipificación de las conductas de fraude informático como delito) se revelan como medios adecuados de control *a posteriori* del riesgo proviniente del fraude informático.

4º Aunque todavía se puede calificar de incipiente en el mercado asegurador la oferta de pólizas destinadas a cubrir el riesgo de fraude informático, queremos destacar en estas conclusiones algunas características de dicha oferta. Como ya hemos indicado la cobertura del riesgo de fraude informático suele producirse a través de la denominada póliza integral bancaria, al ser el sector de bancos y cajas, hasta ahora, el principal demandante de este tipo de cobertura. El hecho de que para asegurar el riesgo de fraude informático se recurra a un apéndice o complemento de la póliza integral bancaria para instituciones financieras, no debe hacer pensar que éstas son las únicas instituciones expuestas al citado riesgo. En síntesis recogemos lo que

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

puede constituir materia de generalizado interés, es decir, los riesgos sobre los que se proporciona seguro:

a) Alteraciones de datos almacenados electrónicamente, de programas y/o de elementos físicos de un sistema informático.

   Pérdidas económicas directas sufridas en planes de pensiones, planes de jubilación, fondos de inversión y otros productos de ahorro-inversión que resulten directamente de una manipulación de ordenadores. El autor podrá ser cualquier persona que a través de una manipulación informática (alteración de datos, de programas y/o de rutinas) haya conseguido que el plan de pensiones, u otro producto de pasivo, sufra una pérdida o haya obtenido un beneficio económico indebido para él o para un tercero.

b) Transferencias electrónicas de fondos realizadas en atención a una comunicación fraudulenta. Cubre el robo de cualquiera de los fondos del asegurado en una cuenta abierta en una institución financiera producido por la ejecución de una orden (instrucción electrónica, telegráfica, por cable, teletipo) de transferencia fraudulenta.

c) Fraudes en transferencias iniciadas via voz. El asegurado transfiere fondos confiando en instrucciones iniciadas por voz (por ejemplo órdenes en banca telefónica).

d) Para instituciones financieras se suele añadir expresamente una cláusula relativas a pérdidas exclusiva y directamente causadas por uno o más actos deshonestos o fraudulentos de manipulación informática de cualquiera de los empleados del asegurado y que tienen como resultado un beneficio económico indebido para éstos.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

5º Inmersos como estamos en la sociedad de la información, contando con un vehículo de publicación de información y de comercio electrónico de la potencia de la red mundial Internet, en su aplicación más conocida

Worl-Wide-Web, controlar (física, lógica y jurídicamente) los posibles ataques a que pueda verse sometida la información almacenada en sistemas conectados a la Red o que viaja por esta red mundial, es hoy una necesidad ineludible.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

PROPUESTA DE SEGURO CONTRA FRAUDE INFORMATICO

1. a) Razón social del Banco.

   b) Nombre y actividad principal de todas las Compañías subsidiarias y/o filiales a incluir en el presentc seguro.

   c) Fecha de fundación del Banco.

   d) Dirección de la Sede Legal.

2. a) Forma de incorporación (Sociedad cotizada en Bolsa, sociedad privada, empresa estatal, etc.)

   b) Especifiquen todas las entidades o personas que controlen más del 10% de las acciones, bien por valor o derecho a votar.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

c) ¿Ha habido algún cambio importante en el accionariado, fusión o adquisición de otra empresa en los últimos 3 años?

En caso afirmativo, proporcionen detalles de la transacción.

3. Por favor indiquen a continuación:

a) Capital autorizado
b) Capital desembolsado
c) Total de activo
d) Total de depósitos
e) Total de préstamos y descuentos

4. ¿Qué porcentaje de sus ingresos se genera de:

a) Actividades de Banca comercial?
b) Inversión?
c) Operaciones de "Trusts"?
d) Banca al pormenor (servicios al público)?
e) Transacciones en la Bolsa?
f) Transacciones con divisas?
g) "Factoring"?

5. Número total de empleados.

6. Número total de situaciones.

7. Número de centros de procesamiento de datos.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

SECCION B - LA COBERTURA DESEADA

8. a) Indiquen el límite de indemnización y franquicias de su actual póliza de Multirriesgo Bancario.

b) ¿Qué secciones y ampliaciones de cobertura han contratado en la póliza de Multirriesgo Bancario?

c) ¿Con qué Compañía de Seguros tienen suscrita su póliza de Multirriesgo Bancario?

¿A través de qué Agente?

9. a) ¿Qué límite de indemnización y franquicia desean para su póliza de fraude informático?

b) ¿Desean alguna cobertura adicional a la básica de la póliza de fraude informático?

Por ejemplo:
i) Efectos de virus informático
ii) Costes de reconstrucción de programas fraudulentamente modificados
iii) Telefax fraudulento
Etc.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

10. a) ¿Ha rehusado algún suscriptor una solicitud suya para este tipo de cobertura (Multirriesgo Bancario o Fraude Informático)?

b) ¿Ha sido anulada o rechazada la renovación de alguna póliza de este tipo?

En caso afirmativo de (a) ó (b), proporcionen detalles.

11. Especifiquen cualquier recomendación o deficiencia de control detectada por las autoridades bancarias, su auditor externo o un asesor independiente. Adjunten copia de las observaciones y/o recomendaciones junto con la respuesta, por escrito, de su gerencia (detallando las medidas adoptadas, etc.)

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

SECCION C - EXPERIENCIA

12. Detallen brevemente en el recuadro expuesto a continuación todas las pérdidas que hayan sufrido durante los últimos cinco años que involucraran cualquier utilización de sistemas informáticos u operaciones relacionadas con sistemas informáticos, y/o cualquier circunstancia conocida que pudiese dar lugar a una pérdida de este tipo, aunque las pérdidas no estuviesen aseguradas.

Fecha descubrimiento	Situación	Tipo de Pérdida	Cantidad real o estimada

Adjunten detalles de las medidas adoptadas con el fin de evitar la repetición de las pérdidas susodichas.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

SECCION D - DESCRIPCION GENERAL DEL PROCESAMIENTO DE DATOS

13.	Nro. aprox. de transac-ciones diarias	"On Line" o procesa-miento en lotes	Efectuados por banco o por em-presa de servicios	Con acceso electróni-co de per-sonas no empleadas
a) Depósitos a la vista / cuentas co-rrientes				
b) Depósitos comerciales				
c) Depósitos a plazo fijo				
d) Préstamos a personas				
e) Préstamos comerciales				
f) Cartas de crédito				
g) "Trusts" per-sonales				
h) "Trusts" de corporaciones				
i) Transferencia de fondos				
j) Transacciones con divisas				
k) Compensación automatizada de cheques				

../..

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

../..

l) Transferencia de título de valores				
m) Custodia de valores				
n) Gestión de dinero				
o) Misceláneo / Otros				

¿Facilitan Vds. cualquiera de las prestaciones arriba mencionadas para algún banco corresponsal u otra entidad financiera? En caso afirmativo, proporcionen detalles.

14. ¿Su organización de procesamiento de datos está centralizada o descentralizada en las siguientes actividades?

a) Desarrollo de sistemas, compra de software.

b) Operación de sistemas principales incluidos los sistemas de telecomunicaciones.

c) Adquisición y operación de ordenadores pequeños.

d) Informática personal.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

15. Indiquen el porcentaje aproximado de procesamiento efectuado:

a) por empleados del Banco
b) mediante un acuerdo con el Holding
c) mediante un acuerdo con un banco corresponsal
d) mediante un acuerdo con un "joint venture"
e) mediante un acuerdo con una empresa de servicios (que no sea un banco)
f) mediante un acuerdo con una compañía subsidiaria.

SECCION E - PROCEDIMIENTOS GENERALES

16. Encargado de la seguridad de datos.

a) ¿Han designado Vds. algún responsable de la implantación y administración de seguridad de datos?

b) ¿Quién es el jefe inmediato del encargado de la seguridad de datos?

c) ¿Existe un manual escrito de la seguridad de datos estableciendo la política de la empresa y las pautas necesarias para mantener la seguridad de los datos?

17. Auditoría interna de informática.

¿Existe un departamento de auditoría interna de procesamiento electrónico de datos?

En caso afirmativo,

a) ¿Existe un manual escrito de "procedimientos de auditoría y control de informática"?

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

b) ¿Cuántos empleados tiene el departamento?

c) ¿Hay un auditor específicamente entrenado para desempeñar sus actividades de auditoría de sistemas informáticos?

d) ¿Está en vigor algún programa completo y continuo de auditoría?

En el caso de no existir tal programa, detallen el alcance de las auditorías actuales.

e) ¿Se hacen informes por escrito? ¿Para quién?

f) ¿Están los encargados de la auditoría libres de otras responsabilidades? ¿Les está así mismo prohibido introducir datos o instrucciones en el sistema?

18. Auditoría externa.

a) ¿Qué firma efectúa la auditoría externa?

b) i) ¿Con qué frecuencia se efectúa la auditoría externa?

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ii) ¿Se realizan en todas las situaciones incluyendo todos los centros de procesamiento de datos?

De no ser así, ¿qué situaciones son investigadas?

iii) ¿La firma de auditores revisa regularmente sus sistemas de controles internos dando informes por escrito?

iv) ¿Ha hecho la firma de auditores alguna recomendación en lo que se refiere a las actividades de procesamiento de datos que no se haya llevado a cabo?

En caso afirmativo, proporcionen detalles de la recomendación y los motivos por no haberla implantado.

19. Acceso al sistema.

a) ¿Se utilizan palabras clave para distintos niveles en base a las necesidades y autorización del usuario?

b) ¿Se cambian regularmente las palabras clave?

¿Las modifican cuando se producen cambios de personal que tienen conocimiento de dichas palabras clave?

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

20. Comunicaciones.

a) ¿Tienen los terminales limitaciones en lo que respecta al tipo de mensaje que cada usuario pueda recibir o enviar?

b) ¿Se utilizan "Log On Passwords" especiales (distintas de las palabras clave de los usuarios) cuando se conecta un terminal al sistema para permitir verificación de la identidad del terminal?

c) ¿Se utilizan sistemas de encriptar datos?

En caso afirmativo, proporcionar detalles.

d) ¿Utilizan un sistema de software para controlar las telecomunicaciones (por ejemplo, TCAM)?

En caso afirmativo, por favor especifiquen el sistema empleado.

22. Seguridad física.

a) ¿El (Los) centro(s) de procesamiento de datos está(n) separado(s) físicamente de otros departamentos?

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

b) ¿Cuáles de las siguientes protecciones existen en el centro de procesamiento de datos?

i) alarma contra ladrones
ii) televisión de circuito cerrado
iii) sistema de supresión de incendios (Halón, etc.)

iv) vigilantes
v) sistema de control de acceso
vi) otros métodos (detallar)

c) ¿Se utilizan sistemas de control de acceso para restringir el C.P.D. solamente a personas específicamente autorizadas?

Indiquen cuáles de las siguientes medidas están empleadas:

i) Exclusa
ii) Control por TV de circuito cerrado desde las instalaciones centrales de seguridad con grabación de las imágenes
iii) Identificación de personas por los jefes de cada turno
iv) Sistema de tarjetas de identificación controlado por miniordenador

d) ¿Se guarda, por lo menos, una generación de archivos en un lugar seguro remoto alejado del centro principal de procesamiento de datos?

e) ¿Los archivos de cintas o disketes están en una zona restringida separada de otros departamentos?

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

SECCION F - CARACTERISTICAS DEL SISTEMA

23. Ordenadores del asegurado.

De acuerdo con los requerimientos de la póliza, por favor identifiquen todos los sistemas de ordenadores a incluir en el seguro, facilitando detalles de:

a) Fabricante/Marca

b) Modelo/Descripción del C.P.U.

c) Descripción del Sistema Operativo/Software

Si opera más de un C.P.U, por favor indíquen el número.

24. Cajeros automáticos.

a) Indiquen el número de cajeros automáticos operados por el Banco (excluyendo redes compartidas).

b) ¿Participan en una red (4B, SERVIRED, 2000) compartida u operada por otra organización?

En caso afirmativo, indiquen qué red y faciliten detalles al respecto.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

c) ¿Los cajeros están conectados "On Line" a un ordenador central?

25. Sistema de ordenadores de una Compañía de Servicios.

a) ¿Utilizan Vds. alguna persona, asociación u organización para convertir datos originales en datos electrónicos?

En caso afirmativo, indiquen:

i) Nombre de la persona/entidad

ii) Clase de servicios facilitados

b) ¿Existe un contrato por escrito con la Compañía de Servicios?

c) ¿Requieren Vds. que la Compañía de Servicios contrate un seguro de infidelidad? ¿Con qué cantidad mínima?

26. Contratistas independientes.

a) ¿Utilizan Vds. contratistas independientes para la preparación de instrucciones electrónicas para los ordenadores?

b) ¿Existe un contrato por escrito estableciendo los deberes y responsabilidades del contratista?

c) ¿Exigen Vds. que los contratistas suscriban una póliza de infidelidad? ¿Con qué límite mínimo?

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

27. Medios.

¿Almacenan Vds. datos sobre:

a) cintas magnéticas?
b) cintas perforadas?
c) discos magnéticos?
d) tarjetas perforadas?
e) otros, por favor especifiquen

28. Cámara de compensación.

a) ¿Utilizan Vds. un sistema electrónico de compensación de débitos y créditos mediante una cámara de compensación automatizada?

b) ¿Utilizan dicho tipo de sistema para dirigir el depósito de pagos regulares?

c) ¿Existe una conexión "On Line" entre su sistema y la cámara de compensación automatizada?

d) Identifiquen la cámara de compensación automatizada utilizada por Vds.

29. Sistemas de comunicación electrónica.

Indiquen todos los sistemas de comunicación electrónica interbancaria utilizados:

a) FEDWIRE
b) CHIPS
c) SWIFT

../..

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

d) BANKWIRE
e) TELEX
f) TWX
g) TELENET
h) TYMNET
i) Otras redes. Por favor, especifiquen.

30. Sistemas de comunicación con los clientes.

a) ¿Tienen Vds. sistemas "On Line" de gestión de fondos con grandes clientes?

En caso afirmativo, por favor indiquen:

i) el nombre del sistema

ii) descripción breve de los servicios facilitados

iii) descripción breve de la configuración del sistema

iv) número aproximado de clientes contactados

v) copia del contrato entre el cliente y el Banco

vi) copia del manual del usuario.

b) ¿Permiten Vds. acceso electrónico a su sistema a sus clientes mediante:

a) "Bank at Home"?
b) terminales en punto de venta?
c) cajeros automáticos?
d) conexión por telex?
e) otro tipo de conexión con terminales? (Por favor, especifiquen)

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Certificamos que la información y datos facilitados en la presente Proposición de Seguro son exactos.

Aceptamos que los datos aportados en la presente Proposición, junto con cualquier otra información adicional, sirvan de base a la confección de la Póliza.

La Entidad Proponente se compromete a informar a la Compañía Aseguradora sobre cualquier modificación que altere sustancialmente los datos aportados, tanto si ocurren con anterioridad o con posterioridad a la toma de efecto de la Póliza.

La firma de esta Proposición de Seguro no supone obligación alguna por parte del Proponente en concertar definitivamente el Seguro.

Toda la información facilitada será tratada rigurosamente con carácter confidencial.

En Madrid, a de de 1990

Por la Entidad Proponente,

DATARISK

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ANEXO II

PÓLIZA DE LLOYD'S CONTRA DELITOS ELECTRONICOS Y A TRAVES DE ORDENADOR

POR CUANTO el Asegurado nombrado en las condiciones particulares nos ha presentado a nosotros, que hemos suscrito nuestros nombres en este documento (en adelante denominados "los Aseguradores"), un Modelo de Propuesta que se ha convenido sirva de base para este seguro. Todas las estipulaciones de dichas condiciones particulares y el Modelo de Propuesta quedan incorporados a y forman parte de la presente Póliza.

AHORA, NOSOTROS, LOS ASEGURADORES, con sujeción a los términos, exclusiones, limitaciones y condiciones siguientes, nos comprometemos a y convenimos en compensar al Asegurado, en la forma determinada en las Estipulaciones del Seguro, por encima de los importes de las franquicias declaradas aplicables, aquella pérdida financiera directa sufrida en cualquier momento por el Asegurado y descubierta por el Asegurado durante el período de la Póliza, sujeto siempre a los límites de la Póliza fijados en las condiciones particulares.

PONEMOS AHORA EN SU CONOCIMIENTO QUE

(a) Nosotros, los Aseguradores, miembros de los sindicatos cuyos números definitivos indicados en la Lista de Miembros Aseguradores de Lloyd's después mencionada figuran en la tabla adjunta, por la presente nos obligamos, cada uno por su propia parte y no por otra y sólo en relación con su debida proporción, a indemnizar al Asegurado cualquier pérdida financiera directa en la forma que aquí se estipula una vez se demuestre la cuantía de dicha pérdida,

(b) la debida proporción de la que es responsable cada uno de nosotros, los Aseguradores, se determinará haciendo referencia a su participación, tal como aparece en la mencionada Lista, en el importe, porcentaje o proporción del total de dicha pérdida asegurada que se encuentra en la tabla frente al número definitivo del sindicato del que es miembro el Asegurador Y

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(c) la Lista de Miembros Aseguradores de Lloyd's a que se hace referencia anteriormente refleja sus respectivos sindicatos y participaciones, se considera incorporada y formando parte de esta Póliza, ostenta el número especificado en la tabla adjunta y está abierta a la inspección por parte del Asegurado o su/s representante/s en la Oficina Firmante de Pólizas de Lloyd's y se entregará al Asegurado a petición una copia fidedigna de las partes fundamentales de la mencionada Lista certificada por el Director General de la Oficina Firmante de Pólizas de Lloyd's.

EN TESTIMONIO DE LO CUAL el Director General de la Oficina Firmante de Pólizas de Lloyd's lo suscribe con su nombre en representación de cada uno de nosotros.

Director General de la Oficina
Firmante de Pólizas de Lloyd's

Para estampación de la Oficina
Firmante de Pólizas de Lloyd's

C 1983 Sindicato Nº 546 (Modelo 183)

Se ruega al Asegurado lea esta Póliza y la devuelva inmediatamente a los efectos oportunos en caso de encontrarla incorrecta.

Se ruega al Asegurado preste atención especial a cada una de las Estipulaciones del Seguro, Estipulaciones Generales, Definiciones, Exclusiones y Condiciones y Limitaciones de este Seguro.

Deberá mencionarse en todas las comunicaciones el número de Póliza que aparece en la primera línea de las condiciones particulares.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ESTIPULACION DEL SEGURO 1

SISTEMAS DE ORDENADOR

A causa de que el Asegurado haya transferido, pagado o entregado cualesquiera fondos o propiedades o establecido algún crédito, cargado en alguna cuenta o dado algún valor a consecuencia directa de la entrada fraudulenta de datos electrónicos directamente en:

(1) los sistemas de ordenador del Asegurado o

(2) el sistema de ordenador de una oficina de servicios o

(3) un sistema de transferencia electrónica de fondos o

(4) el sistema de comunicaciones de un cliente

o de la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados o que se están manejando dentro de cualquiera de los sistemas mencionados o durante la transmisión electrónica a través de líneas de comunicación de datos a sistemas de ordenador del Asegurado o al sistema de ordenador de una oficina de servicios, actos fraudulentos que hayan sido cometidos por una persona con intención de ocasionar una pérdida al Asegurado u obtener un beneficio económico para sí o para cualquier otra persona.

ESTIPULACION DEL SEGURO 2

INSTRUCCIONES PARA EL ORDENADOR ELECTRONICO

A causa de que el Asegurado haya transferido, pagado o entregado cualesquiera fondos o propiedades o establecido algún crédito, cargado en alguna cuenta o dado algún valor a consecuencia directa de la preparación

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

fraudulenta o la modificación fraudulenta de instrucciones para el ordenador electrónico, actos fraudulentos que hayan sido cometidos por una persona con intención de ocasionar una pérdida al Asegurado u obtener un beneficio económico para sí o para cualquier otra persona.

ESTIPULACION DEL SEGURO 3

MEDIOS Y DATOS ELECTRONICOS

A. A causa de la tentativa, amenaza o destrucción malintencionada de datos electrónicos del Asegurado por cualquier persona mientras estos datos se encuentran almacenados dentro de los sistemas de ordenador del Asegurado o del sistema de ordenador de una oficina de servicios.

B. A causa de que los medios de proceso electrónico de datos resulten extraviados, dañados o destruidos a consecuencia directa de robo, hurto, latrocinio, substracción, traspapelamiento o desaparación misteriosa inexplicable mientras los medios de proceso electrónico de datos se encuentran albergados o depositados dentro de oficinas o locales situados en cualquier lugar o bajo la custodia de una persona designada por el Asegurado para actuar como su mensajero (o una persona que actúa como mensajero o custodio durante una emergencia producida por la incapacidad de ese mensajero designado) mientras los medios de proceso electrónico de datos se encuentran en tránsito en cualquier lugar, tránsito que comienza inmediatamente a la recepción de los medios de proceso electrónico de datos por el citado mensajero

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

y termina inmediatamente a la entrega al receptor designado o a su agente, siempre que el Asegurado sea el propietario de tales medios de proceso electrónico de datos o sea legalmente responsable de la pérdida o el daño en cuestión.

ESTIPULACION DEL SEGURO 4

COMUNICACIONES ELECTRONICAS

A causa de que el Asegurado haya transferido, pagado o entregado cualesquiera fondos o propiedades o establecido algún crédito, cargado en alguna cuenta o dado algún valor fiándose de cualesquiera comunicaciones electrónicas dirigidas al Asegurado que fueran transmitidas o aparenten haber sido transmitidas a través de:

(1) un sistema electrónico de comunicaciones o

(2) una cámara de compensación automatizada o

(3) por telex, TWX o medio similar de comunicación directamente a los sistemas de ordenador del Asegurado o al terminal de comunicaciones del Asegurado y que aparenten haber sido enviadas fraudulentamente por un cliente, cámara de compensación automatizada o institución financiera, pero comunicaciones que no hayan sido enviadas por dicho cliente, cámara de compensación automatizada o institución financiera o que hayan sido modificadas fraudulentamente durante el tránsito físico de los medios de proceso electrónico de datos al Asegurado o durante la transmisión electrónica a través de líneas de comunicación de datos a los sistemas de ordenador del Asegurado o al terminal de comunicaciones del Asegurado.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

ESTIPULACION DEL SEGURO 5

OPERACIONES DE LA OFICINA DE SERVICIOS DEL ASEGURADO

A causa de que un cliente del Asegurado haya transferido, pagado o entregado cualesquiera fondos o propiedades, establecido algún crédito, cargado en alguna cuenta o dado algún valor a consecuencia directa de la entrada fraudulenta, la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados o que están siendo manejados dentro de los sistemas de ordenador del Asegurado o durante la transmisión electrónica a través de líneas de comunicación de datos de los sistemas de ordenador del Asegurado al sistema de ordenador del cliente mientras el Asegurado actúa como oficina de servicios para dicho cliente, actos fraudulentos que hayan sido cometidos por una persona con intención de ocasionar una pérdida al Asegurado o al cliente del Asegurado u obtener un beneficio económico para sí o para cualquier otra persona y de cuya pérdida se considere legalmente responsable al Asegurado.

ESTIPULACION DEL SEGURO 6

TRANSMISIONES ELECTRONICAS

A causa de que un cliente del Asegurado, una cámara de compensación automatizada o una institución financiera haya transferido, pagado o entregado cualesquiera fondos o propiedades, establecido algún crédito, cargado en alguna cuenta o dado algún valor fiándose de cualesquiera comunicaciones electrónicas que aparenten haber sido dirigidas por el Asegurado a su cliente, una cámara de compensación automatizada o una institución financiera

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

que autoricen o confirmen la transferencia, pago, entrega o recepción de fondos o propiedades, comunicaciones que hayan sido transmitidas o aparenten haber sido transmitidas a través de:

(1) un sistema electrónico de comunicaciones o

(2) una cámara de compensación automatizada o

(3) por telex, TWX o medio similar de comunicación directamente a un sistema de ordenador o a un terminal de comunicaciones de dicho cliente, cámara de compensación automatizada o institución financiera y que aparenten haber sido enviadas fraudulentamente por el Asegurado, pero comunicaciones que no hayan sido enviadas por el Asegurado o que hayan sido modificadas fraudulentamente durante el tránsito físico de los medios de proceso electrónico de datos del Asegurado o durante la transmisión electrónica a través de líneas de comunicación de datos de los sistemas de ordenador del Asegurado o de la terminal de comunicaciones del Asegurado y de cuya pérdida se considere legalmente responsable al Asegurado.

ESTIPULACION DEL SEGURO 7

TRANSFERENCIAS INICIADAS POR LA VOZ DEL CLIENTE

A causa de que el Asegurado haya transferido cualesquiera fondos fiándose de las instrucciones de transferencia de fondos iniciadas por alguna voz dirigidas al Asegurado que autoriza la transferencia de fondos en la cuenta de un cliente a otros bancos en favor de personas designadas específicamente por el cliente, instrucciones que fueran cursadas por teléfono a aquellos empleados del Asegurado autorizados específicamente para recibir esas instrucciones en las oficinas del Asegurado y que aparenten haber sido cursadas fraudulentamente por una

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

persona autorizada y nombrada por un cliente para solicitar por teléfono la transferencia de tales fondos, pero instrucciones que no hayan sido formuladas por el mencionado cliente ni por ningún directivo, consejero, socio o empleado de ese cliente o que fueran dadas fraudulentamente por un directivo, consejero, socio o empleado del cliente en cuestión cuya función, responsabilidad o autoridad no le permiten cursar, iniciar, autorizar, validar o autenticar instrucciones de transferencia de fondos iniciadas por la voz del cliente, actos fraudulentos que hayan sido cometidos por esa persona con intención de ocasionar una pérdida al Asegurado o al cliente u obtener un beneficio económico para sí o para cualquier otra persona.

Definición Especial

"Cliente", tal como se utiliza en esta Estipulación del Seguro, significa cualquier sociedad, asociación o trust cliente o entidad comercial similar que tenga un acuerdo escrito con el Asegurado respecto a las transferencias de fondos iniciadas por la voz del cliente.

ESTIPULACIONES GENERALES

Póliza Complementaria

(A) La Póliza de Lloyd's contra delitos electrónicos y a través de ordenador está concebida para servir de póliza complementaria a la Bankers Blanket Bond (seguro combinado de fianzas) del Asegurado y pretende cubrir el delito relacionado con ordenadores, conforme se define en las Estipulaciones del Seguro, que no está cubierto por el seguro combinado de fianzas del Asegurado. Habida cuenta de que determinados Aseguradores que aseguran la Póliza de Lloyd's contra delitos electrónicos y a través de ordenador pueden estar asegurando también el seguro combinado de fianzas del Asegurado, bien por un seguro principal, seguro de exceso u otro seguro o reaseguro contributivo y de que su intención no es incrementar ni duplicar su cobertura al Asegurado, queda convenido que esta póliza no se considerará cobertura de exceso o coaseguro.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Costas Judiciales, Honorarios de Letrados y Elección de Defensa por los Aseguradores

(B) Los Aseguradores indemnizarán al Asegurado contra las costas judiciales y los honorarios de letrados razonables incurridos y pagados por el Asegurado en la defensa de cualquier pleito o procedimiento legal respecto al que el Asegurado establezca que el acto o actos que se cometieron facultarían al Asegurado a cobrar en virtud de una Estipulación del Seguro de esta Póliza por encima de cualquier franquicia si hubiera resultado de ello alguna pérdida.

Si la cantidad reclamada al Asegurado o la cantidad finalmente pagada, aquella que sea mayor, excediera la franquicia o superara el importe perceptible al amparo de los términos de esta Póliza, las costas judiciales y los honorarios de letrados en semejante pleito o procedimiento legal serán prorrateados entre el Asegurado y los Aseguradores en razón a la responsabilidad potencial de cada parte incluyendo la franquicia.

La cantidad de indemnización que provean los Aseguradores al Asegurado para costas judiciales y honorarios de letrados razonables no excederá el 10% del límite de la Estipulación del Seguro por la que estaría facultado el Asegurado a recuperar su pérdida, indemnización adicional al límite de dicha Estipulación del Seguro.

El Asegurado notificará rápidamente a los Aseguradores la iniciación de cualquier pleito o procedimiento legal y, a petición de los Aseguradores, les facilitará copias de todos los alegatos y demás documentos pertinentes. El Asegurado permitirá a los Aseguradores, a opción de éstos, tomar a cargo la defensa del mencionado pleito o procedimiento legal en nombre del Asegurado a través de letrados elegidos por los Aseguradores. En tal caso, el Asegurado suministrará toda la información y asistencia razonable que los Aseguradores consideren necesarias para la defensa del procedimiento legal.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Si los Aseguradores pagaran costas judiciales y honorarios de letrados por encima de su cuota proporcional de esas costas y honorarios de letrados, el Asegurado reembolsará rápidamente a los Aseguradores el exceso en cuestión.

Persona Designada por el Asegurado

(C) La pérdida sufrida por cualquier persona constituida por el Asegurado a efectos de llevar a cabo determinadas transacciones comerciales y compuesta exclusivamente por sus directivos, funcionarios u otros empleados, será considerada como pérdida sufrida por el Asegurado a todos los fines de esta Póliza.

Sistemas de Ordenador y Oficinas Adicionales -
Consolidación, Fusión o Compra de Activos - Notificación

(D) Si, dentro del período de vigencia de la presente Póliza, el Asegurado estableciera algunas oficinas adicionales o añadiera a los sistemas de ordenador del Asegurado, de forma que no sea mediante consolidación o fusión con o compra de activos de otra institución, esas oficinas o adición a los sistemas de ordenador del Asegurado quedarán automáticamente cubiertas desde la fecha de su establecimiento sin ser necesario notificarlo a los Aseguradores ni pagar prima adicional por el resto del período de la prima. Si, durante el período de vigencia de esta Póliza, el Asegurado consolidara o se fusionara con o comprara activos de otra institución, el Asegurado no dispondrá de la cobertura proporcionada por esta Póliza respecto a la pérdida que:

(a) se haya producido o se produzca en oficinas, locales o

(b) haya sido o pueda ser causada por los activos adquiridos por el Asegurado a consecuencia de tal consolidación, fusión o compra de activos o adquisición a menos que el Asegurado

(i) notifique por escrito a los Aseguradores la propuesta consolidación, fusión o compra de activos con anterioridad a la fecha propuesta de entrada en vigor de la consolidación, fusión o compra de activos o adquisición y

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(ii) obtenga el consentimiento escrito de los Aseguradores para extender la cobertura proporcionada por esta Póliza a las oficinas o locales adicionales y

(iii) pague a los Aseguradores una prima adicional calculada prorrateadamente desde la fecha de la consolidación, fusión o compra de activos hasta el término del período de prima en curso.

Cambio de Control - Notificación

(E) Cuando el Asegurado tenga conocimiento de una transferencia de sus acciones en circulación con derecho a voto que dé lugar a un cambio de control del Asegurado, cursará notificación escrita a los Aseguradores con un preaviso de 30 días haciendo constar:

(a) los nombres de los transferentes y los transferidos (o los nombres de los propietarios beneficiales si las acciones están registradas a otro nombre) y

(b) el número total de acciones de las que sean propietarios los transferentes y los transferidos (o los propietarios beneficiales) tanto inmediatamente antes como después de la transferencia y

(c) el número total de acciones en circulación con derecho a voto.

Tal como se utiliza en esta Estipulación General, control significa el poder para determinar la gestión o la política del Asegurado en virtud de la propiedad de las acciones con derecho a voto. Todo cambio en la propiedad de las acciones con derecho a voto que dé lugar a la propiedad directa o indirecta por un accionista o un grupo de accionistas afiliados del diez por ciento (10%) o más de las acciones en circulación con derecho a voto del Asegurado, se presumirá da lugar a un cambio de control a efectos de la notificación necesaria.

La omisión de la notificación que se requiere producirá la terminación de la cobertura de esta Póliza con efecto a la fecha de la transferencia de acciones respecto a cualquier pérdida en la que se vea implicado el transferido.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Asegurado Conjunto

(F) Si estuvieran cubiertos por esta Póliza dos o más Asegurados, el Asegurado nombrado en primer lugar actuará por todos ellos. El pago efectuado por los Aseguradores al Asegurado nombrado en primer lugar en relación con la pérdida sufrida por algún Asegurado liberará totalmente a los Asegurados de cara a esa pérdida. Si el Asegurado nombrado en primer lugar cesa de estar cubierto por esta Póliza, se considerará Asegurado nombrado en primer lugar al Asegurado nombrado a continuación. El conocimiento que posea cualquier Asegurado o el descubrimiento realizado por él constituirá conocimiento o descubrimiento para la totalidad de los Asegurados a todos los efectos de esta Póliza. La responsabilidad de los Aseguradores por la pérdida o pérdidas sufridas por todos los Asegurados no excederá la cantidad de la que hubieran sido responsables los Aseguradores si un Asegurado hubiera sufrido todas o cada una de las pérdidas.

CONDICIONES Y LIMITACIONES

SECCION 1 DEFINICIONES

(a) "Sistemas de Ordenador del Asegurado" significa los sistemas de ordenador propiedad de, arrendados u operados por el Asegurado.

(b) "Terminal de Comunicaciones" significa teletipo, teleimpresor o terminal de visualización de imágenes.

(c) "Sistema de Ordenador" incluye un ordenador y todas las instalaciones de entrada, salida, proceso, almacenamiento y comunicación que estén conectadas a ese dispositivo y estén controladas por una copia única del sistema operativo contenido dentro del dispositivo. Las librerías de medios fuera de línea se consideran parte de dicho sistema de ordenador.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(d) "Sistemas de Comunicación del Cliente" significa aquellos sistemas de comunicaciones declarados en la propuesta escrita a los Aseguradores que facilitan a los clientes del Asegurado acceso directo a los sistemas de ordenador del Asegurado.

(e) "Sistema Electrónico de Comunicación" significa las operaciones de comunicación electrónica por Fedwire, Sistema de Pagos Interbancarios de la Cámara de Compensación (SHIFT), Sociedad para la Telecomunicación Financiera Internacional en todo el Mundo (SWIFT), Bankwires y sistemas de comunicación interbancarios automatizados similares declarados en la propuesta escrita a los Aseguradores.

(f) "Instrucciones para el ordenador electrónico" significa programas de ordenador, datos o informes convertidos en un formulario utilizabÍe en un sistema de ordenador para actuar sobre datos electrónicos.

(g) "Datos electrónicos" significa los datos o la información convertidos en un formulario utilizable en el sistema de ordenador y que está almacenado en medios de proceso electrónico de datos para su uso en programas de ordenador.

(h) "Medios de proceso electrónico de datos" significa las fichas perforadas, cintas magnéticas, cintas perforadas o discos magnéticos u otros medios de gran capacidad en los que se registran datos.

(i) "Sistemas de transferencia electrónica de fondos" significa aquellos sistemas que operan cajeros automáticos o terminales en los puntos de venta e incluyen cualesquiera redes o instalaciones compartidas para dicho sistema en las que participa el Asegurado.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(j) "Comprobantes de adeudo" significa los instrumentos otorgados por un cliente del Asegurado y que éste retiene que, en el curso regular del negocio, se consideran como comprobantes de deuda del cliente frente al Asegurado y que incluyen registros de cargos y cuentas a cobrar.

(k) "Oficina de servicios" significa una persona física, asociación o sociedad autorizada por acuerdo escrito para prestar servicios de proceso de datos utilizando sistemas de ordenador.

(l) "Servicio de ordenador de oficina de servicios" significa los sistemas de ordenador pertenecientes a, arrendados u operados por una oficina de servicios.

SECCION 2 EXCLUSIONES

Quedan excluidos de esta póliza:

(a) La pérdida resultante de cualquiera de los riesgos cubiertos por la póliza bancaria del Asegurado.

(b) La pérdida causada por un empleado identificable del Asegurado o por una persona o personas en colusión con algún empleado del Asegurado.

A los fines y efectos de la presente póliza, se considera que el conocimiento previo por algún empleado de que una persona o personas que no son empleados del Asegurado han cometido o cometerán un acto fraudulento, constituye colusión cuando ese empleado evite intencionada o deliberadamente que el conocimiento llegue a oidos del Asegurado. No se considerará ni constituirá colusión si un empleado evita que ese conocimiento llegue a oidos del Asegurado por causa de amenaza de daño físico a alguna persona o de producir daños a los locales o propiedades del Asegurado.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(c) La pérdida de ingresos potenciales incluyendo, pero sin limitación, intereses y dividendos.

(d) La pérdida indirecta o consiguiente de cualquier naturaleza o los daños de cualquier tipo por los que pueda considerarse legalmente responsable al Asegurado con excepción de los daños compensatorios directos derivados de una pérdida cubierta por la presente póliza.

(e) La responsabilidad asumida por el Asegurado merced a acuerdo cubierto por cualquier contrato a menos que esa responsabilidad hubiera sido imputada al Asegurado incluso en ausencia de tal acuerdo.

(f) Los costos, honorarios y demás gastos incurridos por el Asegurado al establecer la existencia o el importe de la pérdida cubierta por esta póliza.

(g) La pérdida debida a motín o conmoción civil o la pérdida debida a poder militar, naval o usurpado, guerra o insurrección salvo que dicha pérdida se produzca en tránsito en las circunstancias expuestas en la Estipulación del Seguro nº 3 y salvo que en el momento de iniciarse ese tránsito no se tuviera conocimiento del motín, conmoción civil, poder militar, naval o usurpado, guerra o insurrección por parte de cualquier persona que actuara por el Asegurado al iniciar dicho tránsito.

(h) (1) Toda pérdida o destrucción o daño sufrido por una propiedad, cualquiera que sea, o toda pérdida o gasto, cualquiera que sea, resultante o derivado de ellos o alguna pérdida consiguiente o

(2) Toda responsabilidad legal de cualquier naturaleza originada o producida o derivada directa o indirectamente de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(i) radiaciones ionizantes o contaminación por radioactividad procedente de algún combustible nuclear o de algún residuo nuclear procedente de la combustión de combustible nuclear

(ii) las propiedades radioactivas, tóxicas, explosivas o de otro tipo peligroso de cualquier montaje nuclear explosivo o componente nuclear del mismo

(i) La pérdida resultante de una amenaza

(1) de causar daño físico a alguna persona, excepto la pérdida de medios de proceso electrónico de datos o de datos electrónicos en tránsito bajo la custodia de una persona que actúe como mensajero siempre que cuando se iniciara dicho tránsito el Asegurado no tuviera conocimiento de tal amenaza o

(2) de causar daños a las propiedades o locales del Asegurado

(j) La pérdida de medios de proceso electrónico de datos o de datos electrónicos mientras se encuentren en el correo o en poder de un transportista de alquiler que no sea una compañía de vehículos blindados.

(k) La pérdida de datos electrónicos o de medios de proceso electrónico de datos excepto lo estipulado en la Sección 7 de las Condiciones y Limitaciones.

(l) La pérdida resultante directa o indirectamente de

(i) instrucciones o avisos escritos o

(ii) instrucciones o avisos telegráficos o por cable o

(iii) instrucciones o avisos verbales a través del teléfono a menos que esté cubierta por la Estipulación del Seguro 7.

(m) La pérdida resultante directa o indirectamente de instrumentos negociables, documentos de títulos o instrumentos escritos falseados, alterados o fraudulentos utilizados como

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

documentación fuente en la preparación de medios de proceso electrónico de datos o tecleados manualmente en un terminal de datos.

(n) La pérdida de instrumentos, títulos, documentos o instrumentos escritos negociables excepto los convertidos en datos electrónicos y sólo en esa forma convertida.

(o) La pérdida resultante directa o indirectamente del acceso a cualquier información confidencial incluyendo, pero sin limitación, la información comercial, los programas de ordenador o la información del cliente de carácter secreto.

(p) La pérdida o el daño causado por incendio.

(q) La pérdida resultante de fallo mecánico, construcción defectuosa, error de diseño, defecto oculto, uso o desgaste, deterioro gradual, alteración eléctrica, fallo de los medios de proceso electrónico de datos o avería o cualquier mal funcionamiento o error en la programación o errores u omisiones en el proceso.

(r) La pérdida resultante directa o indirectamente de la preparación o modificación fraudulenta de instrucciones para el ordenador electrónico salvo que esté cubierta por la Estipulación del Seguro 2.

(s) La pérdida debida a la entrada de datos electrónicos en un terminal electrónico autorizado de un sistema de transferencia electrónica de fondos o un sistema de comunicaciones del cliente por parte de un cliente u otra persona a quien se haya autorizado el acceso al mecanismo de autenticación del cliente.

(t) La pérdida resultante de características fraudulentas contenidas en instrucciones para el ordenador electrónico desarrolladas para venderlas o que se venden a varios clientes en el momento de su adquisición a un vendedor o asesor.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

LIMITE DE RESPONSABILIDAD/NO ACUMULACION DE RESPONSABILIDAD

SECCION 3

La responsabilidad total de los Aseguradores en razón a cualquier pérdida o pérdidas o serie de pérdidas causadas por actos u omisiones de alguna persona, tanto identificable o no, o por actos u omisiones en los que participe o esté implicada esa persona (y considerando todas las pérdidas como un sólo suceso hasta su descubrimiento), no excederá del límite de indemnización de la Estipulación del Seguro aplicable determinado en las condiciones particulares y si, y sólo en este caso, si no existieran directa o indirectamente tales actos u omisiones, la responsabilidad total de los Aseguradores en razón a cualquier pérdida o pérdidas o serie de pérdidas derivadas del mismo caso de fraude, no excederá el límite de indemnización de la Estipulación del Seguro aplicable determinado en las condiciones particulares.

Si fueran de aplicación varias Estipulaciones del Seguro, la responsabilidad total de los Aseguradores no excederá el límite de indemnización cubierto por una de las Estipulaciones del Seguro aplicables determinado en las condiciones particulares y en ninguna circunstancia se acumulará cada límite de indemnización cubierto por Estipulaciones del Seguro separadas.

En el supuesto de que alguna pérdida estuviera cubierta por varias coberturas o Estipulaciones del Seguro, el máximo a pagar por dicha pérdida no excederá el mayor importe previsto por cualquier cobertura o Estipulación del Seguro.

Con sujeción a cuanto antecede, el pago de la pérdida reducirá la responsabilidad respecto a otras pérdidas descubiertas durante cada año de esta póliza y será aplicado al agotamiento del límite acumulado de la póliza.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Con independencia del número de años en que se mantenga vigente esta póliza y del número de primas que deban pagarse o se hayan pagado, la responsabilidad de los Aseguradores no se acumulará en cantidades de año a año o de período a período.

LIMITE ACUMULADO DE LA POLIZA

SECCION 4

Ninguna pérdida excederá el límite de indemnización determinado en las condiciones particulares y, durante cada año de la póliza, el importe total de todas las pérdidas cubiertas por una o varias Estipulaciones del Seguro no excederá el límite acumulado de la póliza a que se hace referencia en el punto 6 de las condiciones particulares.

DESCUBRIMIENTO

SECCION 5

La presente póliza se aplica a la pérdida descubierta por el Asegurado durante el período de la póliza. El descubrimiento se produce cuando el Asegurado tiene conocimiento de hechos que harían suponer a una persona razonable que se ha producido o se producirá una pérdida cubierta por la Póliza, aún cuando no se conozca en ese momento la cuantía exacta o los detalles de la pérdida.

La notificación al Asegurado de una reclamación real o posible por una tercera parte que alegue que el Asegurado es responsable en circunstancias que, de ser ciertas, darían lugar a una pérdida en virtud de esta póliza, constituye descubrimiento.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

SECCION 6

(a) El Asegurado notificará la pérdida a los Aseguradores en el momento más inmediato posible, no superior a 30 días, después de descubierta la misma.

(b) El Asegurado suministrará a los Aseguradores la prueba de la pérdida, debidamente juramentada con toda clase de detalles, dentro de los 6 meses siguientes al descubrimiento.

(c) No se iniciarán procedimientos legales para el cobro de pérdida alguna antes de expirados 60 días después de presentar a los Aseguradores la prueba de la pérdida original o después de expirados 24 meses desde el descubrimiento de dicha pérdida, si bien se iniciará cualquier acción o procedimiento de cobro en razón a cualquier sentencia dictada contra el Asegurado en algún pleito mencionado en la estipulación sobre costas judiciales y honorarios de letrados, o para recuperar los honorarios de letrados pagados en ese pleito, dentro de los 24 meses siguientes a la fecha en que la sentencia y el pleito sean firmes.

(d) En caso de que alguna ley que controle la interpretación de esta póliza prohibiera alguna limitación incorporada en la misma, esa limitación se considerará enmendada de forma que equivalga al período mínimo de limitación contemplado por la ley.

(e) Esta póliza sólo proporciona cobertura en beneficio del Asegurado. Nadie que no sea el Asegurado nombrado podrá incoar pleito, acción o procedimientos legales.

(f) El Asegurado notificará a los Aseguradores, en el momento y en la forma prescritos en esta póliza, cualquier pérdida del tipo cubierto por los términos de la póliza tanto si los Aseguradores son responsables o no de ella y, a petición de

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

los Aseguradores, la cursará acompañada de una breve declaración indicando los datos referentes a la pérdida.

EVALUACION

SECCION 7

Toda pérdida de dinero o pérdida pagadera en dinero, será pagada, a opción del Asegurado, en la moneda del país en que se sufrió la pérdida o en dólares de los Estados Unidos de América equivalentes a la misma, determinados a la tasa de cambio vigente en el momento del pago de la pérdida.

Títulos

Los Aseguradores liquidarán en especie su responsabilidad cubierta por esta póliza a consecuencia de pérdida de cualesquiera títulos o, a opción del Asegurado, pagarán al Asegurado el coste de sustitución de tales títulos determinado por el valor de mercado de los mismos en el momento de la liquidación. En el caso de pérdida de privilegios de suscripción, conversión o amortización por causa de la pérdida de títulos, el importe de esa pérdida será el valor de tales privilegios inmediatamente anterior a la expiración de los mismos. Si no pudieran sustituirse esos títulos o no tuvieran valor de mercado cotizado o si dichos privilegios no tuvieran valor de mercado cotizado, su valor será determinado mediante acuerdo o arbitraje.

Si la cobertura aplicable a esta póliza estuviera sujeta a una franquicia deducible y/o su importe no fuera suficiente para indemnizar totalmente al Asegurado por la pérdida de títulos por la que se presenta reclamación al amparo de la póliza, la responsabilidad de los Aseguradores estará limitada al pago o a la duplicación de aquellos títulos que tengan valor igual al importe de la cobertura aplicable.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Medios de proceso electrónico de datos

En caso de pérdida de o daño a medios de proceso electrónico de datos utilizados por el Asegurado en su negocio, los Aseguradores sólo serán responsables en virtud de esta póliza cuando esos medios sean reproducidos realmente por otros medios de proceso electrónico de datos de la misma clase o calidad y, en tal caso, nada más que del coste de los medios en blanco más el coste de la mano de obra para la transcripción real o la copia de los datos que hayan sido facilitados por el Asegurado al objeto de reproducir los medios de proceso electrónico de datos, con sujeción, desde luego, al límite de indemnización aplicable.

Otras propiedades

En caso de pérdida de o daño a cualquier propiedad que no sea dinero, títulos o medios de proceso electrónico de datos, los Aseguradores sólo serán responsables del valor real en efectivo de esa propiead. Los Aseguradores podrán, a elección suya, pagar el valor real en efectivo de dicha propiedad o sustituirla o repararla. Si no se llegara a acuerdo entre los Aseguradores y el Asegurado en cuanto al valor en efectivo o a la conveniencia de la reparación o sustitución, se recurrirá a arbitraje.

Datos electrónicos

En caso de pérdida de datos electrónicos, los Aseguradores sólo serán responsables en virtud de esta póliza cuando esos datos sean reproducidos realmente por otros datos electrónicos de la misma clase y calidad y nada más que del coste de la mano de obra para la transcripción real o la copia de los datos que hayan sido facilitados por el Asegurado al objeto de reproducir los datos electrónicos, con sujeción, desde luego, al límite de indemnización aplicable.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

No obstante, si no pudieran reproducirse estos datos electrónicos y los mismos representaran títulos o instrumentos financieros que tengan valor, incluyendo comprobantes de adeudo, la pérdida se evaluará conforme se indica en los párrafos referentes a títulos y otras propiedades de esta Sección.

CESION, SUBROGACION, COBRO, COOPERACION

SECCION 8

(a) En el supuesto de pago en virtud de esta póliza el Asegurado hará entrega, si así lo solicitaran los Aseguradores, de una cesión de aquellos derechos, título e interés y causas de acción del Asegurado que éste tenga contra cualquier persona o entidad hasta el límite del pago de la pérdida.

(b) En el supuesto de pago en virtud de esta póliza los Aseguradores se subrogarán los derechos de cobro del Asegurado contra cualquier persona o entidad hasta el límite de dicho pago.

(c) Los cobros, tanto si los efectúan los Aseguradores o el Asegurado, se aplicarán netos de gastos de cobro, primero, a la satisfacción de la pérdida del Asegurado por encima del importe pagado en virtud de la póliza, segundo, a los Aseguradores en concepto de reembolso de las cantidades pagadas en liquidación de la reclamación del Asegurado y, tercero, al Asegurado en satisfacción de cualquier franquicia deducible. El cobro debido a pérdida de títulos, conforme se determina en el segundo párrafo de la sección 7, o el cobro procedente de reaseguro y/o indemnización de los Aseguradores, no se considerará cobro tal y como aquí se utiliza.

(d) A petición de los Aseguradores y en los momentos y lugares razonables designados por los Aseguradores, el Asegurado:

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(1) someterá al examen de los Aseguradores y los suscribirá bajo juramento y

(2) presentará para ser examinados por los Aseguradores todos los documentos pertinentes y

(3) cooperará con los Aseguradores en todas las materias referentes a la pérdida.

(e) El Asegurado otorgará todos los documentos y prestará asistencia para asegurar a los Aseguradores los derechos y las causas de acción que aquí se contemplan. Después del descubrimiento de la pérdida el Asegurado no llevará a cabo nada que perjudique estos derechos o causas de acción.

LIMITE DE RESPONSABILIDAD EN VIRTUD DE ESTA POLIZA Y SEGURO ANTERIOR

SECCION 9

Con respecto a cualquier pérdida determinada en la Sección 3 de esta póliza que sea recuperable o se recupere en su totalidad o en parte al amparo de algunas otras fianzas o pólizas emitidas por los Aseguradores al Asegurado o a cualquier antecesor en interés del Asegurado y que hayan terminado, hayan sido canceladas o dejadas expirar y en las que no haya expirado el período de descubrimiento en el momento en que se descubre esa pérdida, la responsabilidad total de los Aseguradores en virtud de esta póliza y de otras fianzas o pólizas no excederá, en conjunto, el importe asegurado para esa pérdida o el importe al alcance del Asegurado en razón de esas otras fianzas o pólizas, limitado por los términos y condiciones de las mismas, por cualquier pérdida si el último importe fuera mayor.

Si la cobertura de esta póliza invalidara total o parcialmente la cobertura de alguna otra fianza o póliza de seguro emitida por un Asegurador ajeno a los Aseguradores y que haya terminado, haya sido cancelada o dejada expirar, los Aseguradores serán responsables en virtud de esta póliza, respecto a cualquier pérdida sufrida con

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

anterioridad a dicha terminación, cancelación o expiración y descubierta dentro del período permitido por tal otra fianza o póliza para el descubrimiento de la pérdida, sólo de la parte de pérdida cubierta por esta póliza que exceda del importe recuperable o recuperado en razón a la pérdida cubierta por la otra fianza o póliza mencionada, con independencia de cuanto esa otra fianza o póliza contenga en sentido contrario.

OTRO SEGURO O INDEMNIZACION

SECCION 10

Con excepción de lo dispuesto en la Estipulación General A, la cobertura proporcionada por esta póliza se aplicará sólo como exceso sobre cualquier seguro válido y perceptible tanto si ese otro seguro se declara como principal, contributivo, de exceso o contingente o sobre indemnización obtenida por el Asegurado o por una compañía de vehículos blindados o por otra entidad en cuyos locales se produjo la pérdida o que empleaba a la persona causante de la pérdida o el mensajero que transportaba los medios de proceso electrónico de datos. Como seguro de exceso, esta póliza no se aplicará ni contribuirá al pago de ninguna pérdida hasta que se haya agotado el importe del otro seguro o indemnización mencionados, quedando entendido y convenido que el Asegurado será reembolsado por esta póliza hasta el límite de la diferencia entre la cantidad recuperable de aquel otro seguro o indemnización y la cantidad de la pérdida real recuperable de otro modo al amparo de esta póliza.

PROPIEDAD

SECCION 11

La presente póliza se aplicará a la pérdida de propiedades y a la pérdida de medios de proceso electrónico de datos y datos electrónicos pertenecientes al Asegurado, poseidos por el Asegurado

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

en cualquier capacidad o de los que el Asegurado sea legalmente responsable. Esta póliza servirá para el uso y beneficio exclusivo del Asegurado nombrado en las Declaraciones.

FRANQUICIA DEDUCIBLE

SECCION 12

Los Aseguradores sólo serán responsables del importe en que exceda cualquier pérdida la franquicia deducible correspondiente a la Estipulación del Seguro aplicable a esa pérdida, con sujeción al límite de indemnización para esa Estipulación del Seguro.

TERMINACION O CANCELACION

SECCION 13

Esta póliza se considerará terminada o cancelada en su totalidad (a) 60 días después de recibida por el Asegurado una notificación escrita de los Aseguradores respecto a su deseo de terminar o cancelar la póliza o (b) a la recepción inmediata por los Aseguradores de una solicitud escrita del Asegurado para terminar o cancelar la póliza o (c) con carácter inmediato al hacerse cargo del Asegurado un síndico u otro liquidador o funcionarios estatales o federales o (d) con carácter inmediato al hacerse cargo del Asegurado otra institución. Los Aseguradores reembolsarán, a petición, al Asegurado la prima no devengada computada en base a prorrateo si esta póliza fuera terminada o cancelada o reducida mediante notificación o a instancias de los Aseguradores o si fuera terminada o cancelada con arreglo a lo estipulado en la subsección (c) o (d) de este párrafo. Los Aseguradores reembolsarán al Asegurado la prima no devengada computada en base a primas reducidas si esta póliza fuera terminada o cancelada o reducida mediante notificación o a instancias del Asegurado.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Esta póliza se considerará terminada o cancelada en relación a cualquier oficina de servicios (a) tan pronto como algún Asegurado o algún consejero o directivo que no actúe en colusión con esta persona tenga conocimiento de un acto deshonesto o fraudulento cometido en un momento dado por algún socio, consejero, directivo o empleado de dicha oficina de servicios contra el Asegurado o alguna otra persona o entidad, sin perjuicio para la pérdida de cualquier propiedad que se encuentre entonces en tránsito bajo la custodia de esa persona o (b) 15 días después de la recepción por el Asegurado de una notificación escrita de los Aseguradores en cuanto a su deseo de terminar o cancelar esta póliza respecto a la persona en cuestión.

La terminación de la póliza respecto a cualquier Asegurado pone fin a la responsabilidad ante cualquier pérdida sufrida por el Asegurado que sea descubierta después de la fecha en que surte efecto la terminación.

DERECHOS POSTERIORES A LA TERMINACION O CANCELACION

SECCION 14

En cualquier momento anterior a la terminación o cancelación de esta póliza por los Aseguradores, el Asegurado podrá notificar a los Aseguradores que desea un período adicional no superior a 12 meses que le permita descubrir dentro de él la pérdida sufrida por el Asegurado con anterioridad a la fecha en que surte efecto la terminación o cancelación y pagará por ello una prima adicional.

A la recepción de esta notificación del Asegurado, los Aseguradores darán su consentimiento escrito; en el bien entendido, sin embargo, de que este período de tiempo adicional terminará con carácter inmediato

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

(a) en la fecha en que entre en vigor cualquier otro seguro contratado por el Asegurado, su sucesor en el negocio o cualquier otra parte, que sustituya total o parcialmente el seguro proporcionado por esta póliza, tanto si ese otro seguro ofrece o no cobertura para la pérdida sufrida con anterioridad a su fecha de entrada en vigor o

(b) cuando algún funcionario u organismo estatal o federal o algún síndico o liquidador que intervenga o sea nombrado a tal efecto se haga cargo del negocio del Asegurado

sin ser necesario que los Aseguradores notifiquen la terminación. En caso de que este período de tiempo adicional quede terminado conforme a lo estipulado previamente, los Aseguradores reembolsarán cualquier prima no devengada.

El derecho a comprar este período adicional para el descubrimiento de la pérdida no podrá ser ejercido por ningún funcionario ni organismo estatal o federal ni por síndico o liquidador alguno que intervenga o haya sido nombrado para hacerse cargo del negocio del Asegurado de cara a la operación o a la liquidación del mismo o para cualquier otro fin.

ACCION CONTRA EL CLIENTE Y LA OFICINA DE SERVICIOS

SECCION 15

Esta póliza no proporciona cobertura en beneficio de ningún cliente u oficina de servicios conforme a lo antedicho y, previo pago al Asegurado por los Aseguradores en razón a cualquier pérdida ocasionada por actos fraudulentos o deshonestos cometidos por alguno de los socios, consejeros, directivos o empleados de ese cliente u oficina de servicios, tanto si actúan en solitario o en colusión con otros y, en la medida de dicho pago, el Asegurado hará cesión a los Aseguradores o a uno de los Aseguradores designado por

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

los Aseguradores, de aquellos derechos y causas de acción que pueda tener el Asegurado contra el cliente o la oficina de servicios mencionados por causa de los actos cometidos y el Asegurado otorgará todos los documentos necesarios para asegurar a los Aseguradores o a uno cualquiera de los Aseguradores designado por éstos los derechos que aquí se contemplan.

FRAUDE-GARANTIA

SECCION 16

Si el Asegurado presentara alguna reclamación conociendo que es falsa o fraudulenta por lo que se refiere a su importe o por otro concepto, esta póliza quedará nula y todas las reclamaciones a su amparo quedarán sin efecto; pero ninguna declaración formulada por o en nombre del Asegurado, tanto si está contenida o no en la propuesta, se considerará garantía de nada excepto cuando sea fidedigna según el leal saber y entender de la persona que formula la declaración.

CITACION A JUICIO

SECCION 17

Queda convenido que en caso de que los Aseguradores dejen de pagar alguna cantidad reclamada como debida, los Aseguradores, a solicitud del Asegurado, se someterán a la jurisdicción de cualquier tribunal de jurisdicción competente dentro de los Estados Unidos y cumplirán todos los requisitos necesarios para otorgar jurisdicción a dicho tribunal; todas las materias derivadas de ello se resolverán con arreglo a la ley y a las normas de ese tribunal.

Queda asimismo convenido que podrán entregarse citaciones a juicio a la persona nombrada en las condiciones particulares que esté debidamente autorizada para aceptarlas en representación de los

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Aseguradores y que, en todo pleito entablado contra cualquiera de ellos en virtud de esta póliza, los Aseguradores se someterán a la resolución firme del tribunal o de cualquier tribunal de apelación en caso de que se interponga recurso.

A solicitud del Asegurado, la persona nombrada en las condiciones particulares está debidamente autorizada para comprometerse por escrito ante el Asegurado a comparecer en nombre de los Aseguradores en caso de entablarse pleito.

Además, de conformidad con cualquier disposición de algún estado, territorio o distrito de los Estados Unidos que contemple esta norma, los Aseguradores designan al Inspector, Comisionado o Director de Seguros u otro funcionario especificado a tal efecto en los reglamentos o a su sucesor o sucesores en el cargo, como apoderado auténtico y legítimo a quien puede hacerse entrega de cualquier citación judicial en cualquier acción, pleito o procedimiento incoado por o en nombre del Asegurado a consecuencia de este contrato de seguro y designa al antes mencionado como la persona a quien el aludido funcionario está autorizado a enviar citaciones o una copia fidedigna da las mismas.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

CONDICIONES PARTICULARES

PUNTO 1. POLIZA Nº:

PUNTO 2. NOMBRE DEL ASEGURADO:

Domicilio Principal

PUNTO 3. PERIODO DE LA POLIZA. Del:
Al:

PUNTO 4. PRIMA:

PUNTO 5. MODELO DE PROPUESTA fechado el:
El modelo de propuesta, junto con toda la correspondencia relacionada con él y firmada por o en nombre del Asegurado, servirá de base para el seguro.

PUNTO 6. LIMITE ACUMULADO DE LA POLIZA:

PUNTO 7. Limites de la Póliza

El límite de indemnización cubierto por esta póliza con sujeción a la Sección 3 de las Condiciones y Limitaciones será de

EN EL BIEN ENTENDIDO, sin embargo, que si se indicaran importes inferiores para cada Estipulación del Seguro que aparece a continuación, la responsabilidad de los Aseguradores respecto a la pérdida correspondiente a estas Estipulaciones del Seguro estará limitada a los importes inferiores que se consideren como parte de y no adicionales al límite de indemnización antes mencionado.

Estipulación del Seguro 1
Sistemas de Ordenador

Estipulación del Seguro 2
Instrucciones para el Ordenador Electrónico

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Estipulación del Seguro 3
Medios y Datos Electrónicos

Estipulación del Seguro 4
Sistemas Electrónicos de Comunicación

Estipulación del Seguro 5
Operaciones de la Oficina de Servicios del Asegurado

Estipulación del Seguro 6
Transmisiones Electrónicas

Estipulación del Seguro 7
Transferencias iniciadas por la voz del cliente.

PUNTO 8. Franquicias:

El importe de la franquicia, sujeto a la Sección 12 de las Condiciones y Limitaciones aplicables a la Estipulación del Seguro respectiva es el siguiente:

Estipulación del Seguro 1
Sistemas de Ordenador

Estipulación del Seguro 2
Instrucciones para el Ordenador Electrónico

Estipulación del Seguro 3
Medios y Datos Electrónicos

Estipulación del Seguro 4
Sistemas Electrónicos de Comunicación

Estipulación del Seguro 5
Operaciones de la Oficina de Servicios del Asegurado

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

Estipulación del Seguro 6
Transmisiones Electrónicas

Estipulación del Seguro 7
Transferencias iniciadas por la voz del cliente.

PUNTO 9. CITACION A JUICIO

PUNTO 10. NOTIFICAR PERDIDAS A:

PUNTO 11. SUPLEMENTOS:

Fechado en Londres el

Número definitivo de sindicatos e importe, porcentaje o proporción de la suma total asegurada repartida entre los miembros de esos sindicatos.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

BIBLIOGRAFÍA

ALDAMA BAQUEDAMO: *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 n° 30, 1993, pp. 9 y ss.

ALASTUEY DOBÓN, M.D.: *Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial*. III Congreso Iberoamericano de Informática y Derecho. UNED, Mérida.

ALONSO ROYANO, F.: *Estado de Derecho o Derecho del Estado. (El delito informático)*. Revista General del Derecho, n° 498, 1986, pp. 597 y ss.

AMBROJ MARTÍNEZ, F.: *La Seguridad en un entorno de Intercambio Electrónico de la Información (EDI)*. Revista SIC n° 8, Diciembre 1993, pp. 40 y ss.

AMORY, B.; POULLET, Y.: *Le droit de la prevue face a l'informatique et a la telematique*. Revue Internationale de Droit Compare, n° 2, 1985, pp. 31 y ss.

BACIGALUPO ZAPATER: *Utilización abusiva de cajeros automáticos por terceros no autorizados*. Poder Judicial n° especial IX, 1989.

BAJO FERNÁNDEZ, M.: *Manual de Derecho Penal. Parte Especial. Delitos Patrimoniales y Económicos*. Editorial Ceura, Madrid 1987.

- *El delito de estafa*. En volumen "Comentarios a la legislación penal: la reforma del Código Penal de 1983". Tomo V, vol. 2°, Madrid 1985.

BEAUMONT, J.F.: *Aumenta el robo electrónico en los centros de procesos de datos*. EL PAÍS, 14 de marzo de 1990.

BEQUAI, A.: *Computer Crime*. Heath Lexington Books, Lexington, 1978, pp. 9 y ss.

BIELZA, C.: *El disquete como alternativa a las tarjetas de crédito para dar seguridad a las transacciones en INFOVÍA e INTERNET*. II Congreso Nacional de Usuarios de INTERNET e INFOVÍA. Mundo INTERNET, Libro de Ponencias, Madrid 1997. pp. 443 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

BILEK, A.J.: *Desarrollo de un plan de protección contra el fraude informático*. Revista Banca Española 1988.

BLAS ZULETA, L.: *Delitos Informáticos*, Revista General del Derecho, nº 495, 1985.

BLINN, JAMES D.; SANGREE, CARL H.: *Protección de instalaciones de procesamiento electrónico de datos*. Revista Gerencia de Riesgos, Volumen I, (1983/1984), nº 2, MAPFRE, Madrid, pp. 1-52.

BOBADILLA SANCHO, J.M.; ROMÁN MONZO, J.L.: *Gerencia de Riesgos e Informática*. Revista Gerencia de Riesgos, Volumen VI, (1988/1989), nº 24, MAPFRE, Madrid, pp. 41-48.

BOLAÑOS RAMÍREZ, M.R.: *El Delito Informático como nueva figura jurídica*. Actas del Congreso Iberoamericano de Informática Jurídica. CREI, Madrid 1985.

BORRUSO, R.: *Computer e diritto. Problemi giuridici dell' informatica*. Giuffre Editore, Milán 1988, Tomo II, pp. 269 y ss.

BRIAT, M.: *La Delinquance Informatique: Aspects de droit compare*. VIII Congreso: Le Droit Criminal Face aux Technologies Nouvelles de la Asociation de Editores del Reino Unido, Ed. Económica, París 1986, pp. 263 y ss.

BRIAT, M.: *La fraude informatique: une approche de droit compare*. Revue de Droit Penal et de criminologie, 1985.

BUENO ARUS, F.: *El delito informático*. Actualidad Informática Aranzadi nº 11, Madrid 1994, pp. 1 y ss.

CAMACHO LOSA, L.: *El delito informático*. Gráficas Cóndor, Madrid 1987.

CAMBELL, D.: *The investigation of fraud*. Barry Rose Publishers Lyd., England 1979, pp. 7 y ss.

CARBONEL PINTANEL, J.: *La protección del consumidor titular de tarjetas de pago en la Comunidad Europea*. Ediciones Beramar, Eurolex, Colección de Estudios Internacionales, Madrid 1994.

CARMONA, A.M.: *Economía e Innovación*. Prensa y Ediciones Iberoamericanas, S.L, Madrid 1992, pp. 22 y ss.

CARRACEDO, J.: *Apuntes de la asignatura Arquitectura de Ordenadores I. Parte I*. Departamento de Ingeniería y Arquitectura Telemáticas. Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Universidad Politécnica de Madrid.

CASTAÑO COLLADO, C.: *Tecnología, empleo y trabajo en España*. Alianza editorial, Madrid 1994, pp. 137 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

CASTELLS ARTECHE, M.: *Impacto de las tecnologías avanzadas sobre el concepto de seguridad: Evolución cultural y tecnológica*. FEPRI, Madrid 1987.

CASTILLO JIMÉNEZ, M.C.: *El delito informático*. Congreso sobre Derecho Informático. Universidad de Zaragoza, Zaragoza 1989, pp. 563 y ss.

CEREZO MIR, J.: *Curso de Derecho Penal Español. Parte General*. Volumen I. 3ª edición, Tecnos, Madrid 1985.

CIGNA WORLDWIDE UNDERWRITING GUIDELINES: *Virus Informáticos*. Cigna, UK 8/3/90.

COMER, J.M.: *Corporate fraud*. MCGRAW-HILL BOOKS, CO.LTED. Inglaterra 1977.

CONDE-PUMPIDO TOURON: *Las tarjetas de crédito como instrumento para la comisión de un delito*. Poder Judicial nº especial IX, 1989, pp. 133 y ss.

CORCOY BIDASOLO, M.: *Protección Penal del sabotaje informático. Especial consideración de los delitos de daños*. En volumen: "Delincuencia informática", PPU, Barcelona 1992, pp. 145-176.

CORCOY, M.; JOSHI, U.: *Delitos contra el patrimonio cometidos por medios informáticos*. Revista Jurídica de Cataluña, nº 3, Barcelona 1988.

CZARNOTA, B.; HART, R.J.: *Legal protection of computer programs in Europe: A guide to EC Directive*. Butterworths, London 1991.

C.A.P.A. (COMITE D'ACTION POUR LA PRODUCTIVITE DANS L'ASSURANCE): *Método de evaluación de riesgos en actividades informáticas*. Revista Gerencia de Riesgos. Año VIII (1990/1991), nº 30, MAPFRE, Madrid, pp. 41-42.

CHICKEN, JOHN C.: *Estudio sobre pérdidas informáticas esperadas hasta el año 2000 en la industria aseguradora europea*. Revista Gerencia de Riesgos. Volumen V (1987/1988), nº 2, MAPFRE, Madrid.

DAVARA RODRÍGUEZ, M.A.: *El delito informático*. En volumen *Derecho Informático*. 1ª edición, Aranzadi, Pamplona 1993, pp. 315-362.

- *La informática en la legislación*. Actualidad Informática Aranzadi nº 11, Madrid 1994.

DE LA MATA: *Utilización abusiva de cajeros automáticos: apropiación de dinero mediante tarjeta sustraida a su titular*. Poder Judicial nº especial IX, 1989, pp. 151 y ss.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

DOMAICA MAROTO, J.M.: *Manipulaciones en cajeros automáticos. ¿Realidad o ficción?*. Revista AUSBANC nº 69, Marzo 1996, pp. 40 y 41.

ESTADELLA YUSTE, O.: *La protección de la intimidad frente a la transmisión internacional de datos personales*. Tecnos, Madrid 1995, pp. 105 y ss.

FARRENY, A.: *Europa impotente ante las diferentes posibilidades de fraude informático*. Diario La Vanguardia, Madrid, 4 de abril de 1987.

FERNÁNDEZ GONZÁLEZ, J.: *Mecanismos de seguridad en servicios telemáticos*. Actas SECURMÁTICA 96, Sesión III, Madrid 1996.

- *Seguridad en Redes. Servicios de Seguridad en X.400*. Penta 3. Seguridad Informática. (Pendiente de Publicar).

FERNÁNDEZ GONZÁLEZ, J.; RODRÍGUEZ, A.: *Seguridad en entornos EDIFACT*. Revista SIC nº 8. Diciembre 1993, pp. 45 y ss.

FERNÁNDEZ MASIÁ, E.: *La protección de los programas de ordenador en España*. Tirant Lo Blanch. Serie Monografías nº 52, Valencia 1996, pp. 32 y ss.

FISCALÍA GENERAL DEL ESTADO: *Tipicidad del apoderamiento de tarjetas de crédito y su posterior utilización para sacar dinero*. Nº 42.1, Anuario de Derecho Penal y CC. Penales, Madrid 1989, pp. 289-293.

FROSINI, V.: *Cibernética, Derecho y Sociedad*. Tecnos, Madrid 1982.

GARCÍA PABLOS MOLINA, A.: *El impacto de las tecnologías y medios de información en el derecho penal*. Boletín CITEMA nº 118, 1985, pp. 66 y ss.

- *Informática y Derecho Penal. Implicaciones sociojurídicas de las tecnologías de la información*. CITEMA, Madrid 1984.

GARCÍA RIVAS: *El derecho fundamental a una interpretación no extensiva en el ámbito penal. (Comentario a la sentencia del Tribunal Constitucional 111/1993, de 23 de marzo)*. Revista Jurídica de Castilla La Mancha nº 17, abril 1993, pp. 27 y ss.

GARCÍA RODRÍGUEZ, C.: *Programas de ordenador: perspectiva jurídica y policial*. Revista Actualidad Informática Aranzadi nº 15, Madrid 1995, pp. 1 y ss.

GETE-ALONSO Y CALERA, M.C.: *El pago mediante tarjetas de crédito*. La Ley, Madrid 1990.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

GIL MARTÍNEZ: *Algunos supuestos delictivos de tarjetas de crédito y cajeros automáticos*. Poder Judicial nº especial IX, 1989, pp. 141 y ss.

GIMBERNAT ORDEIG, E.: *Consideraciones sobre los nuevos delitos contra la propiedad intelectual*. Poder Judicial, nº especial sobre nuevas formas de delincuencia. Consejo General del Poder Judicial, Madrid 1989, pp. 351 y ss.

GÓMEZ BENITEZ, J.M.: *Función y contenido del error en el tipo de estafa*. ADPCP, 1985, pp. 335 y ss.

GONZÁLEZ RUS, J.J.: *Aproximación al tratamiento penal de los ilícitos patrimoniales por medios o procedimientos informáticos*. Revista Facultad de Derecho Univ. Complutense, nº 12, Madrid 1986.

- *Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*. Poder Judicial nº especial IX, Madrid 1989, pp. 160 y ss.

GONZÁLEZ SÁNCHEZ, J.; SÁNCHEZ ALONSO, M.: *El problema de la seguridad en INTERNET*. II Congreso Nacional de Usuarios de INTERNET e INFOVÍA. Mundo INTERNET, Sesiones Prácticas, Madrid 1997, pp. 593 y ss.

GUERRA BALIC, J.: *Consideraciones para la regulación penal del delito informático*. Anexos I, Jornadas de Abogacía e Informática. Ilustre Colegio de Abogados de Barcelona, Barcelona 1993.

GUTIÉRREZ FRANCÉS, M.L.: *La criminalidad defraudatoria por medios informáticos en el Anteproyecto de Nuevo Código Penal de 1992*. III Congreso Iberoamericano de Informática y Derecho, UNED, Mérida.

- *En torno a los fraudes informáticos en el derecho español*. Actualidad Informática Aranzadi nº 11, Madrid 1994, pp. 7 y ss.

- *Fraude informático y estafa. (Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos)*. Ministerio de Justicia, Secretaría General Técnica, Madrid 1991.

HEREDERO HIGUERAS, M.: *La Transferencia Electrónica de Fondos en el marco del sector público*. En volumen "Implicaciones socio-jurídicas de las Tecnologías de la Información. Encuentros 1980-1990", CITEMA, pp.479 y ss.

INZA ALDAZ, J.: *Descripción de SET*. II Congreso Nacional de Usuarios de INTERNET e INFOVÍA. Mundo INTERNET, Sesiones Prácticas, Madrid 1997, pp. 49 y ss.

- *Firma electrónica*. II Congreso Nacional de Usuarios

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

de INTERNET e INFOVÍA. Mundo INTERNET, Libro de Ponencias. Madrid 1997. pp. 113 y ss.

- *INFOPISTAS*. Revista Mundo NCR. N° 2, II Etapa, Madrid 1997, pp. 26 y ss.

JAEGER: *La fraude informatique*. Revue de Droit Penal et de Criminologie, 1985.

KALDOR, N.: *A model of economic growth*. The Economic Journal. Vol. LXVII.

KOZOLCHYK, B.: *Cartas de crédito electrónicas*. La Ley. Derecho de los Negocios. Año III. N° 22/23, Madrid 1992, pp. 5 y ss.

KUZNETS, S.: *Crecimiento Económico Moderno: resultados y reflexiones*. Revista Española de Economía. Año VI. N° 1, 1973, pp. 377-397.

LANZI, A.: *Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Italie*. International Review of Penal Law. Vol. 64, 1993, pp. 425 y ss.

MAESTRE ZANGO, J.: *El delito más anónimo*. Cuadernos de seguridad, n° 15, Madrid 6/1989, pp. 11-15.

MARTÍN, W.: *Crime and the computer*. Oxford 1991, pp. 34 y ss.

MATEU DE ROS, R.: *La contratación bancaria telefónica*. Revista de Derecho Bancario y Bursátil. Año XV. N° 62, Abril-Junio 1996, pp. 265 y ss.

MEDINA, M.; BUCH: *Respuesta a incidentes de seguridad*. Revista SIC, n° 22. Año V, Madrid 1996, pp. 46 y ss.

MEHL, C.: *Criminalidad informática*. Tela Versicherung AG., Munich.

MERA FIGUEROA, J.: *Fraude civil y penal*. Ediar Conosur LTDA., Santiago de Chile 1986, pp. 89 y ss.

MERLI, A.: *Il diritto penale dell' informatica: legislazione vigente e prospettive di riforma*. La Giustizia Penale. 1993, pp. 118-128.

MÖHRENSCHLAGER, M.E.: *El nuevo derecho penal informático en Alemania*, en volumen "Delincuencia informática". PPU, Barcelona 1992, pp. 99-144.

MÖHRENSCHLAGER, M.E.: *Tendencias de política jurídica en la lucha contra la delincuencia relacionada con la informática. (Las recomendaciones de la OCDE, las deliberaciones del Consejo de Europa, y el nuevo Derecho alemán)*. En volumen "Delincuencia informática". PPU. Barcelona. 1992. pp. 47-64.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

MORÁN VIÑE, J.M.: *Datos informáticos: Riesgos y Prevención.* Revista Gerencia de Riesgos, volumen IV, nº 2 (1986/1987), MAPFRE.

MORANT RAMON, J.L.; RIBAGORDA GARNACHO, A.; SANCHO RODRÍGUEZ, J.: *Seguridad y Protección de la Información.* Editorial Centro de Estudios Ramón Areces, S.A. Colección de Informática, Madrid 1994. pp. 91 y ss.

MUÑOZ CIDAD, C.: *Estructura Económica Internacional. Introducción al Crecimiento Económico Moderno.* Biblioteca Cívitas Economía y Empresa. CÍVITAS, Madrid 1992. pp. 75 y ss.

MUÑOZ CONDE, F.: *Derecho Penal. Parte especial.* Tirant lo Blanch. Valencia 1988, pp. 239 y ss.

- *La ideología de los delitos contra el orden socioeconómico en el Proyecto de Ley Orgánica de Código Penal.* CPC Nº 16, 1982.

- *La reforma de los delitos contra el patrimonio.* Documentación Jurídica. Monográfico sobre la PANCP. Volumen I, 1983.

MURILLO DE LA CUEVA, P.L.: *La protección de los datos personales ante el uso de la informática en el Derecho español (I).* Revista de Estudios Doctrinales, Nov.-Dic. 1992, Estudios de Jurisprudencia. Año I, nº 3, pp. 7-60.

NEWMANN, P.G.: *Fraud by computer.* Communications of the ACM. Vol. 35 nº 8, 1992, pp. 154 y ss.

NIMMER, R.T.: *The law of computer tecnology.* New York 1985.

NYCUM: *The criminal law aspects of computer abuse: Part I - State penal laws.* Rutgers Journal of Computers and Law, 5. 1976.

ORTI VALLEJO, A.: *Derecho a la intimidad e informática. (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada).* Editorial Comares, Granada 1994.

PARKER: *Computer crimes.* Scribners, New York 1980.

PEREDA HUELVES, J.; FERNÁNDEZ REBOLLOS, B.J.: *Servicios de seguridad ofrecidos por las tarjetas inteligentes.* Revista SIC nº 21. Año V, Madrid 1996.

PERET, D.: *Delito Informático.* Legislación informática. Madrid.

PEREZ GÓMEZ, J.M.: *La organización empresarial ante los fraudes informáticos.* Revista ESIC Market. 1988.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

PESO NAVARRO, E. del: *La Auditoría Informática como medio de prevención contra el delito informático*". III Encuentro sobre Derecho e Informática, U.P.C.O. ICADE, Madrid 1989, pp. 137 y ss.

- *Problemática Jurídica de las Tarjetas de Crédito*. En volumen "Implicaciones socio-jurídicas de las Tecnologías de la Información. Encuentros 1980-1990", CITEMA. pp. 505 y ss.

PESO NAVARRO, E. del; RAMOS GONZÁLEZ, M.A.: *Confidencialidad y Seguridad de la información: La LORTAD y sus implicaciones socioeconómicas*. Ediciones Díaz de Santos, Madrid 1994.

PUERTA, LUIS: *Las tarjetas de crédito en el campo penal*. Poder Judicial nº especial IX, 1989, pp. 97 y ss.

RIBAS ALEJANDRO, J.: *Comercio electrónico en INTERNET: aspectos jurídicos*. II Congreso Nacional de Usuarios de INTERNET e INFOVÍA. Mundo INTERNET, Libro de Ponencias, Madrid 1997, pp. 9 y ss.

- *Los delitos informáticos en el futuro Código Penal*. Anexos Primeras Jornadas de Abogacía e Informática. Ilustre Colegio de Abogados de Barcelona. Barcelona 1993.

RODRÍGUEZ DEVESA, J.M.: *Derecho Penal Español. Parte General*. Dykinson. 9ª edición, Madrid 1985.

- *Derecho Penal Español. Parte Especial*. Dykinson. 9ª edición, Madrid 1983.

RODRÍGUEZ ZARCO, J.M.: *El fraude informático*, en volumen "Manual de prevención del fraude". ESABE, Madrid 1991.

ROMEO CASABONA, C.M.: *Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos*. Poder Judicial nº especial IX, 1989, pp. 109 y ss.

- *Los delitos de daños en el ámbito informático*. Cuadernos de política criminal nº 43, 1991, pp. 91 y ss.

- *Delitos patrimoniales en conexión con sistemas informáticos de telecomunicación*. Congreso sobre Derecho informático. Universidad de Zaragoza. Zaragoza 1989.

- *El derecho penal y las nuevas tecnologías*. Revista del Foro Canario nº 87, Enero-abril 1993, pp. 195 y ss.

- *Las nuevas tecnologías de la información: un nuevo reto para el Derecho*. Telos, 1988.

- *Poder informático y seguridad jurídica*. FUNDESCO, Madrid 1988.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

- *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*. Poder Judicial nº 31, Septiembre 1993, pp. 163 y ss.

- *La utilización abusiva de tarjetas de crédito*. Separata de Revista de Derecho Bancario y Bursátil. Nº 26, Madrid 1987.

RUIZ VADILLO, E.: *Algunas consideraciones sobre la delincuencia informática*. Anexos I Jornada de Abogacía e Informática, Ilustre Colegio de Abogados de Barcelona. Barcelona 1993.

- *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad*. Econ. Jornadas de Estudio sobre nuevas formas de delincuencia. Consejo General del Poder Judicial, Madrid 1988, pp. 53 y ss.

SALAS CLAVER, J. de: *Comercio Electrónico: bases para una interpretación jurídica*. Revista AUSBANC, nº 82, Abril 1997, pág. 26.

SANDOVAL GONZÁLEZ, J.: *Dinero electrónico*. II Congreso Nacional de Usuarios de INTERNET e INFOVÍA. Mundo INTERNET, Sesiones Prácticas, Madrid 1997, pp. 649 y ss.

SCALA ESTALELLA, J.J.: *Validez legal de los soportes informáticos*. En volumen "Implicaciones socio-jurídicas de las Tecnologías de la Información. Encuentros 1980-1990". CITEMA, pp. 443 y ss.

SIEBER, U.: *Documentación para una aproximación al delito informático*. En volumen "Delincuencia Informatica". Promociones y Publicaciones universitarias, Barcelona 1992. pp. 65-9.

- *The international handbook on computer crime*. John Wiley and Sons, Chichester, 1986.

- *Criminalidad Informática: peligro y prevención*. En volumen "Delincuencia Informática". PPU. Barcelona 1992. pp. 13-45.

SOLÁ, J.; AMENGUAL, C.:*INTERNET como canal de distribución*. II Congreso Nacional de Usuarios de INTERNET e INFOVÍA. Mundo INTERNET, Libro de Ponencias, Madrid 1997, pp. 307 y ss.

SOLER DE ARESPACOCHAGA, J.A.: *La seguridad informática. Planes de contingencia*. Revista Gerencia de Riesgos, año X (1992/1993), nº 38, MAPFRE, Madrid, pp. 19-32.

STAMPA BRAUN, J.M.; BACIGALUPO, E.: *La reforma del Derecho Penal Económico español*. Revista Jurídica de Cataluña. Nº extra sobre el Proyecto de Código Penal. Barcelona 1980.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

TAMAMES, R.: *Estructura Económica Internacional*. Alianza Editorial, Madrid 1990, pp. 191 y ss.

TELA IBÉRICA: *Póliza Infotronic*. Tela Ibérica, Madrid 1992.

TELA VERSICHERUNG: *Previsión de siniestros. Seguro de equipos electrónicos*. Prevención de siniestros. Edición 2 V-4, Munich.

- *Seguro de criminalidad informática*. Tela Versicherung.

- *Boletín de siniestros. Siniestros en portadores de datos*. Boletín de Siniestros. Edición 2 A-6, Munich.

- *Prevención de siniestros. Seguridad de datos. Consejos para usuarios de PC's*. Prevención de siniestros. Edición 2 V-12, Munich.

- *Seguridad del Software*. Tela Versicherung.

TÉLLEZ VALDÉS, J.: *Aspectos legales de los virus informáticos*. III Congreso Iberoamericano de Informática y Derecho. UNED, Mérida.

- *Terrorismo por computadora*. Revista Informática y Derecho. UNED, Mérida 1992, pp. 177 y ss.

- *Derecho Informático*. Universidad Nacional Autónoma de México, México 1987, pp. 105 y ss.

TEODORO I SADURNÍ, J.: *Intercambio electrónico de datos (EDI)*. Ministerio de Obras Públicas, Transportes y Medio Ambiente. Secretaría General de Comunicaciones. Dirección General de Telecomunicaciones. Madrid 1994, pp. 15 y ss.

TIEDEMANN, K.: *Poder económico y delito*. Ariel Derecho, Barcelona 1985.

TORTRAS, C.: *El delito informático*. ICADE, Madrid 1989.

TUDANCA, L.A.: *Seguro de cobertura contra el fraude informático*. VIPS.

U.S., DEPARTMENT OF JUSTICE: *Criminal Justice Resource Manual of Computer Crime*. Washington 1979, pp. 9 y ss.

VALLVE, J.: *El EDI, una herramienta de estrategia comercial*. Super ARAL lineal. Año XXVII, nº 1191, Marzo 1994, pp. 8 y ss.

VAQUERO, J.A.: *Aplicación informática para la gerencia de riesgos y seguros de la empresa*. Revista Gerencia de Riesgos, Año IX (1991/1992) nº 36, MAPFRE, Madrid.

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

VÁZQUEZ-QUINTANA, J.M.: *La Interactividad en los medios de comunicación*. En volumen "Apuntes de la Sociedad Interactiva. Autopistas Inteligentes y Negocios Multimedia". Colección Encuentros 2. FUNDESCO, Cuenca 1994, pp. 409 y ss.

VILARIÑO PINTOS, E.: *El delito informático. Derecho comparado y aspectos jurídico-internacionales*. Editorial Tecnos. Colección Hacia un Nuevo Orden Internacional Europeo, pp. 807 y ss.

VILLAR PALASÍ, J.L.: *Aspectos Jurídicos y Políticos de la Tele mática*. Revista de Derecho Administrativo nº 19. Oct.-Dic. 1978, pp. 501 y ss.

VOLGYES, M.R.: *The investigation, prosecution and prevention of computer crime: A State of the art review*. Computer/Law Journal n. 2, 1980, pp. 385 y ss.

YAMAGUCHI, A.: *Computer crimes against information technology in Japan*. International Review of Penal Law. Vol. 64, Würzburg 1993, pp. 434 y ss.

* * * * * *

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

MAP 913.1-DOM-CON
23208

© FUNDACIÓN MAPFRE
Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE