REVISTA DE DERECHO PENAL Y CRIMINOLOGÍA, 2.ª Época, n.º 19 (2007), págs. 217-243

RESPUESTA PENAL FRENTE A FRAUDES COMETIDOS EN INTERNET: ESTAFA, ESTAFA INFORMÁTICA Y LOS NUDOS DE LA RED

JAVIER GUSTAVO FERNÁNDEZ TERUELO
Profesor titular de Derecho penal.
Universidad de Oviedo

1. Las conductas fraudulentas en Internet

Una de las manifestaciones lesivas más intensamente desarrolladas en la Red es precisamente aquella consistente en la producción fraudulenta de perjuicios patrimoniales a terceros. Esto es lo que básicamente podría englobarse bajo el concepto —no necesariamente jurídico— de *estafa*. La aparición de internet y su potencialidad como instrumento comercial de intercambio (vg. comercio electrónico), junto al desarrollo en su ámbito de actividades de carácter económico o financiero (vg. banca *on-line*) ha determinado, como consecuencia necesaria, el acceso al canal de quienes pretenden obtener un lucro ilícito. En efecto, el modelo clásico tradicional de fraude ha encontrado también acomodo en la Red con infinidad de fórmulas más o menos ingeniosas. Así, en este medio se han desarrollado peculiares manifestaciones fraudulentas, algunas de las cuales no pueden ser perseguidas, desde un punto de vista jurídico, recurriendo al modelo clásico típico de estafa. El fenómeno se ha visto potenciado por el desconcierto inicial, la escasa adaptación al medio y la limitada percepción del riesgo de algunos usuarios, circunstancias aprovechadas por quienes pretenden desarrollar el fraude[1].

[1] La característica afectación a múltiples sujetos-víctimas de este tipo de conductas plantea la posible consideración, cuando parte de los mismos no estén identificados, de la figura del «*sujeto pasivo masa*» (art. 74.2 CP); sin embargo, debe tenerse en cuenta el carácter restrictivo con el que opera la jurisprudencia respecto al mismo, así como la tendencia a recurrir en estos supuestos al tipo agravado de estafa por *la entidad del perjuicio ocasionado* (art. 250.6 CP).

2. Fórmulas específicas de fraude

Resumimos a continuación cuales son algunas de las principales fórmulas de fraude utilizadas en el medio internet, para más adelante ver si todas ellas son susceptibles de castigo penal a través de las diferentes formas de estafa presentes en el Libro II del Código Penal español. Son muchas las posibles categorizaciones[2]; sin embargo, con objeto de simplificar ese objetivo creo que es conveniente utilizar un criterio inicial basado en el método utilizado para cometer el fraude.

2.1. Obtención de los datos o claves de acceso (incluídos números y claves de tarjetas de crédito o débito) a determinados servicios y uso indebido de los mismos

2.1.1. Sustracción de las claves de acceso sin el conocimiento de la víctima (spyware)

Entre las fórmulas significativas de fraude están aquellas mediante las cuales se logra la **sustracción de datos que permiten la suplantación de personalidad de la víctima**; así se obtienen por ejemplo las claves bancarias, datos de tarjetas de crédito o claves de acceso a determinadas páginas o servicios; dichos datos serán posteriormente utilizados para conseguir disposiciones o ventajas económicas en favor del autor de la sustracción o de terceros. Esta fórmula implica normalmente el acceso al sistema operativo de la víctima a través de la red (sin olvidar tampoco una posible sustracción física de las claves de acceso a determinados servicios).

El acceso a distancia al PC de la víctima puede tener lugar a través de múltiples vías. Sin embargo, en la actualidad dichos datos suelen obtenerse a través de *spyware* o archivos espía, que son pequeñas aplicaciones que se consiguen introducir en el PC de la víctima, y cuyo objetivo es el envío, a un lugar exterior (habitualmente al PC del defraudador), de datos del sistema donde están instalados (normalmente claves de acceso), mediante la utilización subrepticia de la

[2] Citamos la clásica distinción referida al delito informático general entre: a) Introducción de datos falsos *(data diddling)* o alteración, supresión u ocultación de los ya introducidos. b) Manipulaciones en el programa. c) Manipulaciones en el sistema de salida de datos u *output*; vid por todos, CHOCLÁN MONTALVO J. A., «Fraude informático y estafa por computación», *en Internet y Derecho penal, Cuadernos de Derecho Judicial*, CGPJ, 2001, p. 330 y ss.

conexión a la red, sin el conocimiento del usuario. En la práctica, las principales fórmulas empleadas por el software espía para propagarse son troyanos[3] o bombas lógicas[4] que se descargan desde Internet y se instalan a través de controles *ActiveX* procedentes de fuentes poco fiables o inseguras o mediante la instalación de programas *freeware* o *shareware* que los llevan ocultos. Los más utilizados, lo que hacen es registrar todo lo que los usuarios teclean en su ordenador *(keyloggers)*, si bien otros más complejos acceden a dicha información sin necesidad de que el usuario teclee nada, abriendo puertos y accediendo a la información cuando el usuario ingresa en un enlace determinado. De este modo, el defraudador se hace con información personal, como pueden ser los datos bancarios y las claves de acceso que serán posteriormente utilizados para realizar transferencias a su favor o en favor de un tercero.

2.1.2. Obtención fraudulenta de las claves: Es la propia víctima la que, sin saberlo, hace llegar al defraudador los datos necesarios para realizar las transacciones (phishing)

Los datos de acceso necesarios para el fraude también pueden conseguirse haciendo que sea la propia víctima la que los comunique directamente al defraudador, recurriendo para ello a específicas formas de engaño. En concreto, la más utilizada en la actualidad es la técnica del *phishing*.

El llamado ***phishing*** es una manifestación de la llamada ingeniería social[5] y consiste normalmente en el envío de correos electrónicos que, aparentando provenir de fuentes fiables —normalmente entidades bancarias—, adoptan su imagen corporativa: con logotipos,

[3] Un *troyano* o caballo de Troya actual es un programa que aparentemente efectúa una función útil para quién lo ejecuta, pero que en realidad realiza una función que el usuario desconoce, generalmente dañina.

[4] Las *bombas lógicas* son similares a los troyanos, pero mientras que un troyano se activa cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un fichero con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo sin activarse y por tanto sin que nadie note un funcionamiento anómalo.

[5] La *ingeniería social* consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. El atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad, por parte de personas relacionadas de una u otra forma con el sistema, para poder engañarlas en beneficio propio.

imágenes y textos que han sido recogidos del sitio real. Para ello suelen incluir un enlace que lleva a páginas web falsas con aspecto casi idéntico al de la entidad a la que suplantan, de tal manera que el usuario no desconfíe de ella. Una vez allí se pide al cliente que introduzca, como ha hecho otras veces en la web auténtica, sus contraseñas o números de tarjeta de crédito con lo que sus datos ya están en manos ajenas y listos para ser utilizados con fines delictivos (normalmente se le amenaza además con que, de no hacerlo, las cuentas serán canceladas o bloqueadas). En algunas ocasiones ni siquiera se redirige a la víctima a la web falsa, sino que el mismo mail contiene un pequeño formulario en el que se pide al usuario que introduzca sus datos secretos de acceso y operaciones. A veces, dependiendo del navegador que use, se llega a modificar la barra de direcciones, de tal modo que al seleccionarla se accede a la web suplantada. El envío suele ser masivo e indiscriminado y de este modo algunos de los receptores resultan ser efectivamente clientes de la entidad suplantada.

Aunque en la mayoría de los casos analizados hasta la fecha, lo que se hace es suplantar la imagen corporativa y la web originaria de entidades bancarias, se han detectado otras fórmulas como las siguientes: encuestas falsas en nombre de organismos oficiales que tienen por objeto recoger datos personales de los usuarios que decidan participar en la misma; páginas falsas de recargas de móviles con tarjeta de crédito o de venta de diversos productos (a precios sospechosamente baratos), en los que, una vez obtenidos los datos personales y de la tarjeta, la página enseña algún tipo de error o indica que la operación no se ha podido realizar; presuntos compradores que le piden al vendedor datos bancarios para pagarle el producto que tiene a la venta, los cuales serán utilizados para realizar transacciones ilícitas, etc.

Una variante del *phishing* aparece constituida por el ***pharming***, que consiste en manipular las direcciones DNS *(Domain Name Server*) que utiliza el usuario. Los servidores DNS son los encargados de conducir a los usuarios a la página que desean ver. Pero a través de esta acción, quien pretende defraudar consigue que las páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca *on-line*. Tan sólo es necesario modificar un pequeño archivo llamado *host,* que puede encontrarse en cualquier máquina que funcione bajo Windows y que utilice Internet Explorer para navegar por Internet. A través del «pharming», cuando el usuario teclea en su navegador la dirección de la página a la que quiere acceder, es reenviado a otra creada por el *hacker* que tiene el mismo aspecto que la original. Así, el internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo al defraudador.

En el caso de la **banca *on-line* (tanto si los datos son sustraídos como enviados por la propia víctima)** los autores del fraude, con las claves en su poder, suelen abrir de modo simultaneo una cuenta bancaria a la que remiten el dinero mediante transferencia «online». Estas cuentas se situarán normalmente en sucursales bancarias de terceros países a donde acuden de modo inmediato a retirar el dinero. Para ejecutar estafas de importantes partidas de dinero los autores suelen fraccionar las transferencias a diferentes entidades bancarias, aunque muy próximas geográficamente, de manera que el cobro se puede materializar en un breve espacio de tiempo. También es frecuente la intervención de terceros, éstos, conocidos con el nombre de «mulas» o «muleros», reciben el dinero en sus cuentas bancarias personales, y tras quedarse con la comisión, lo remiten a donde les han indicado los autores del fraude (normalmente giros postales al extranjero). Suelen ser captados a través de Internet mediante diversas fórmulas; por ejemplo supuestas y engañosas ofertas de trabajo, para lo que tienen que rellenar un cuestionario que se ofrece en una página web de la supuesta empresa contratante y facilitar un número de cuenta en la que se van a ingresar transferencias de supuestos clientes ofreciendo, a cambio, una comisión o porcentaje del dinero recibido.

Desde un punto de vista penal, debemos plantearnos si puede ser sancionada la conducta de quienes ponen sus cuentas al servicio de los defraudadores a cambio de dinero (como hemos dicho denominados «muleros»). La respuesta no es sencilla. En primer lugar, habrán de distinguirse aquellas situaciones en las que los mismos desconocen totalmente que están colaborando con la realización de un acto delictivo de las que lo conocen o, más frecuentemente, se lo imaginan (actuando por tanto con dolo eventual). En el primer caso, pensemos que el autor del fraude suele captar a los muleros mediante falsas ofertas de trabajo en las que los mismos deben realizar algún tipo de tarea, por lo que el porcentaje de la transferencia que se queda en su poder se presenta como el pago por el trabajo realizado. Pues bien, obviamente en tal supuesto debe descartarse cualquier tipo de responsabilidad. Más dudas se suscitan en el segundo (conocimiento de la posible actuación delictiva). En tal caso, no creo que pueda plantearse la posible presencia de un delito de receptación. Aparentemente el mulero actúa con ánimo de lucro y, con conocimiento de la comisión de un delito contra el patrimonio, ayuda a los responsables a aprovecharse de los efectos del mismo; sin embargo en nuestro caso, el delito en cuestión no está aún consumado, sino que precisamente la recepción por parte del mulero es el último momento necesario para determinar la consumación (perjuicio o pérdi-

da patrimonial derivado de la disposición patrimonial). En cuanto a una posible participación delictiva, el acto a valorar radicaría en la entrega de un número de cuenta propio, sabiendo de forma cierta o admitiendo la posibilidad de que la misma sea utilizada para cometer el fraude. A mi juicio se tratará normalmente de una aportación idónea para fundamentar la imputación objetiva de una acción de cooperación necesaria o de complicidad, al haber removido obstáculos que hubieran impedido o dificultado la acción del autor. Sin embargo, no debe olvidarse que la posibilidad de admitir la participación con dolo eventual en el delito de estafa no es pacífica[6].

2.2. Dialers (conexiones telefónicas fraudulentas)

Entre las modalidades fraudulentas más dañinas se encuentra el **uso de programas de marcado telefónico *(dialers)***, los cuales establecen una conexión telefónica a redes mediante un número de tarificación adicional de altísimo coste y en las que, normalmente, no se informa adecuadamente, o se ocultan de modo específico, las consecuencias de su instalación. Los marcadores telefónicos se suelen descargar mediante un fichero ejecutable (extensión *.exe*) o incluso a través de un control *ActiveX*. Lo importante es que en muchas ocasiones no se informa de que van a instalar un programa en el disco duro y/o hacer modificaciones en el sistema (como crear conexiones de acceso telefónico a redes), con lo que confundirán a usuarios con pocos conocimientos en la materia. Lo más habitual es que el usuario ni siquiera tenga noticia de la instalación que se realiza en su ordenador, para lo cual se llega a deshabilitar el sonido del modem, al objeto de que las futuras conexiones a los números de tarificación adicional pasen desapercibidas. Desde un punto de vista jurídico, estos programas sólo pueden considerarse lícitos cuando adviertan de un modo claro y nítido, algo muy poco frecuente en la práctica, de los cambios que van a hacer en el sistema y los costes en que incurre el usuario al utilizarlos. Debe en todo caso resaltarse, que esta fórmula empieza a ser superada gracias a la progresiva sustitución de las conexiones telefónicas a través del modem por las de cable, pues los *dialers* no afectan a usuarios que no accedan a Internet mediante RTB (Red Telefónica Básica) o RDSI.

[6] Favorable a dicha posibilidad en nuestra doctrina es, entre otros, CEREZO MIR J., *Curso de Derecho Penal Español. Parte General. Teoría jurídica del delito*, tecnos, Madrid, 2001, tomo III, p. 234.

2.3. Fraudes en operaciones de comercio electrónico

Muchas de las conductas fraudulentas se producen en operaciones de comercio electrónico; se trata básicamente de fraudes en la entrega de la cosa (por parte del vendedor) o en el pago del precio (por parte del comprador). Por lo tanto, de las mismas pueden ser víctimas tanto los consumidores como las empresas que lícitamente se dedican a este comercio, e incluso las entidades bancarias que ponen a disposición del presunto vendedor los instrumentos de pago[7]. Conviene recordar que el miedo de los consumidores a ser engañados a la hora de comprar a través de la Red se ha presentado siempre como el principal obstáculo para el desarrollo del comercio electrónico[8] y que sin embargo el mismo, según un reciente informe de la Asociación Española de Comercio Electrónico (AECE), afecta más a las empresas que a los propios usuarios.

Las fórmulas habituales de fraude consisten en el envío o la entrega de un bien que no reúne las características en base a las cuales se realizó su oferta y adquisición o incluso en la falta de envío o entrega del mismo, utilizando como formas de pago el pago anticipado o contra reembolso[9]. Desde el punto de vista del adquirente, la mayoría de los supuestos fraudulentos se basan en la ausencia de pago y suplantación de la personalidad del comprador real, haciendo soportar los cargos del mismo a una tercera persona que desconoce la operación.

---

[7] Supuesto como el contemplado en la SAP Barcelona de 15 de septiembre de 2005 (ARP 2006\27), relativa a una condena de un sujeto por delito de estafa por la contratación con dos entidades bancarias del servicio de venta por internet (TPV virtual) para desarrollar su actividad comercial, que es usado fraudulentamente a través de la introducción de datos de tarjetas de crédito a las que efectúan cargos indiscriminadamente.

[8] A finales de 2005, el porcentaje de internautas ya ascendía hasta el 46.6% de la población de 15 y más años en península, Baleares y Canarias, lo que supone una cifra de 17.233.433 individuos. La evolución respecto al año 2004 (40,3%), recoge un incremento en el porcentaje de internautas en más de 6 puntos, o lo que es lo mismo, un crecimiento de un 15,6% sobre los datos del año anterior. Por su parte, el número de internautas compradores alcanza, en 2005, la cifra del 25,1%. En términos absolutos pasamos de 3.959.000 internautas compradores en el año 2004, a 4.326.790 en el año 2005. La incorporación neta de más de 367.000 nuevos internautas compradores, supone un crecimiento de más de un 9,2%. La cifra de 4,3 millones de internautas compradores, significa que el 12% 11,7% de la población española de más de 15 años ha comprado en el pasado año por Internet. Estudio sobre comercio electrónico B2C 2006 <http://observatorio.red.es/estudios/documentos/B2C2006.pdf> [Consulta: 1 marzo 2007]

[9] Entre ellas se encuentra el llamado «phishingcar», en el cual se pide al internauta una señal por la venta de un coche que nunca se efectuará.

2.4. Envío de mails fraudulentos

Nos referimos ahora a los supuestos en los que el correo electrónico es un simple medio de contacto con la víctima (como lo podría ser una conexión telefónica o el correo ordinario) para desarrollar diversos fraudes. Se trata por ejemplo de la llamada «estafa nigeriana», consistente en el envío masivo de *emails* que ofrecen a los remitentes diferentes opciones de ganar dinero: premios de lotería, negocios «fáciles» (normalmente para recibir el dinero, primero hay que desembolsar una cantidad destinada a sufragar supuestos tramites previos); mensajes de correo electrónico en los que se comunica al receptor que se le hará un cargo en su tarjeta de crédito por una compra nunca efectuada; en el mismo se suministra a la vez un número de teléfono para cualquier aclaración que implica una conexión internacional en la que se mantiene a los afectados durante varios minutos; etc.

3. Problemas derivados de la ausencia de medidas preventivas y nuevas soluciones técnicas

3.1. Medidas preventivas frente a los fraudes en operaciones de comercio electrónico (garantías jurídicas)

Una de las fórmulas de pago en la adquisición de bienes por internet más segura para el consumidor es aún hoy la tarjeta de crédito, ya que ésta otorga a su titular un amplio margen de maniobra sobre la base del derecho que tiene a solicitar la anulación del cargo[10].

En concreto, el art. 46 de la **Ley de Ordenación del Comercio Minorista** —LOCM— (Ley 7/1996, de 15 de enero, modificada por la Ley 47/2002, de 19 de diciembre) reconoce un derecho al titular de la tarjeta de pago, consistente en exigir la inmediata *anulación del cargo* cuando el pago se haya realizado *fraudulenta o indebidamente utilizando el número de una tarjeta de pago*[11]. El fundamento del art. 46 es la protección del titular de la tarjeta en cuya cuenta se haya hecho indebidamente el cargo

[10] Sobre los diferentes medios de pago a los que se recurre en este ámbito puede verse, MATA MARTÍN R., «Algunos aspectos de la delincuencia patrimonial en el comercio electrónico», en *El comercio electrónico*, Edisofer, Madrid, 2001, p. 454 y ss.

[11] Artículo 46. «*Pago mediante tarjeta. 1. Cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago,*

del precio de una compraventa a distancia, ya sea debido a un error o al uso fraudulento de la tarjeta por un tercero. Para proceder a la referida anulación no se requiere siquiera acreditar la existencia de error o fraude[12]. El vendedor tiene la obligación de anular inmediatamente el cargo en el supuesto de que el comprador lo solicite sin entrar en más consideraciones, si bien, para evitar abusos, la anulación no implica automáticamente la resolución del contrato, con lo que el vendedor podrá hacer uso de las posibilidades que le otorga el art. 1124 CC[13].

Además, el art. 44 LOCM concede al consumidor un *derecho de desistimiento en las ventas a distancia*, en virtud del cual se le faculta para poner fin de forma unilateral dentro de un plazo (de 7 días hábiles), a la relación contractual. Una garantía más en favor del comprador y otra prueba de lo importante que es en estos casos actuar correctamente, devolviendo en el plazo indicado el bien recibido si no es de nuestro agrado; obsérvese, por ejemplo, como la SAP A Coruña de 24 de mayo de 2001 (JUR 2001\226263), en aplicación del principio *in dubio pro reo*, revoca una sentencia condenatoria por el delito de estafa (envío de un paquete contra reembolso conteniendo dos cajas y folletos, en vez de la consola comprada por internet por el denunciante), en base a los siguientes argumentos: «*Ciertamente no descartamos la hipótesis o la probabilidad de un engaño y fraude a través de internet y un envío contrareembolso que estuviese vacío desde su origen, pero esto hay que probarlo fuera de toda duda racional cosa no lograda en el caso enjuiciado*»[14]. La devolución del paquete hubiese conseguido invertir la carga de la prueba, haciéndose cargo el

---

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 la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución reconocido en el artículo 44 y, por 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». [Artículo modificado por la ley 47/2002, de 19 diciembre].

[12] PACHECO CAÑETE M., «La protección del consumidor una vez perfecto el contrato en las ventas de productos a distancia a través de internet», en *La Ley*, núm. 5184, 2000, p. 1 y ss.

[13] Artículo 1124 CC: «*La facultad de resolver las obligaciones se entiende implícita en las recíprocas, para el caso de que uno de los obligados no cumpliere lo que le incumbe. El perjudicado podrá escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y abono de intereses en ambos casos. También podrá pedir la resolución, aun después de haber optado por el cumplimiento, cuando éste resultare imposible*».

[14] Absolución por los mismos motivos ante un caso similar (condena en primera instancia por falta de estafa): SAP Zaragoza de 6 de mayo de 2005 (JUR 2005\159787).

comprador, a tenor de lo dispuesto en la ley 26/1991 (ley de contratos celebrados fuera de los establecimientos mercantiles), únicamente de los gastos de devolución[15].

Otra situación que en la práctica puede plantearse es que, tras la pérdida o sustracción de la tarjeta por parte de su titular, **los datos contenidos en la misma (número de tarjeta, fecha de caducidad o CCV) sean utilizados fraudulentamente para realizar transacciones en internet**. Pues bien, con carácter general, el titular de la tarjeta ha de ser resarcido por el banco de los gastos ocasionados por el uso fraudulento de la misma por parte de terceros. Determinadas «Recomendaciones de la Unión Europea» han dado lugar a la adopción de un Código de Buenas Prácticas, que limita la responsabilidad del usuario. El Banco de España ha indicado de forma insistente que son los bancos quienes han de cubrir los fraudes que sufran los usuarios cuando éstos han sido víctimas de un uso fraudulento de sus tarjetas y siempre que hayan actuado diligentemente, esto es, denunciando la pérdida o sustracción de la misma lo antes posible. Muchas entidades bancarias intentan exonerarse de responsabilidad alegando negligencia por parte de los clientes. Sin embargo, han de hacerse cargo de cubrir el importe de lo defraudado en su totalidad. Únicamente en el caso de que el fraude se haya realizado antes de que el propietario de la tarjeta lo denuncie, el cliente debe hacerse cargo de los primeros 150 euros defraudados. En caso de no ser atendidos, el cliente puede interponer una reclamación ante el mismo banco y ante el Servicio de reclamaciones del Banco de España.

La protección del usuario o consumidor es en todo caso notablemente más intensa que la de los titulares de los negocios *on-line*. Respecto a estos últimos, lo normal será seguir un criterio restrictivo similar al utilizado por la jurisprudencia con relación al delito de estafa. Obsérvese por ejemplo como un supuesto de utilización fraudulenta de tarjeta de crédito (o de los datos en ella recogidos) causando un grave perjuicio a una agencia de viajes *on-line* fue considerado atípico por asumir la empresa «riesgos excesivos» en la venta a través de la web (*haber colaborado de forma relevante la víctima en su propia victimización*): SAP Baleares de 15 de octubre de 2004 (JUR 2004\276745): «*De ninguna garantía disponía la mercantil de autos, que le condujera plausiblemente a la convicción de que el titular de las tarjetas había contratado y, por ende, se había comprometido al pago de los servicios demandados, por lo que no parece que el puro hecho de activar la tarjeta y comprobar el límite de su cobertura*

[15] Cfr. PACHECO CAÑETE M., «La protección del consumidor», *loc. cit*., p. 3.

pueda, objetivamente, erigirse en estímulo eficaz como para acceder a una prestación cuyo buen fin era, en principio, una pura incógnita, asumiendo por consiguiente un intolerable riesgo, desde el fin de protección de la norma, que absolutamente nada (excepto una ciega confianza) justificaba el asumirlo»; en el mismo sentido, la sentencia del Juzgado número 3 de Málaga de 19 de diciembre de 2005: «*Huelga decir que ninguna de esta conductas fue llevada a cabo por los acusados los cuales compran a través de una página web un reproductor de DVD y para el pago del precio designan un número de tarjeta VISA de la que es titular otra persona totalmente ajena a los hechos. Por ello, no cabe incluir la conducta de los acusados en el párrafo segundo del art. 248 del C.Penal, pues los mismos no manipularon sistema o programa informático alguno sino, cuando se les solicita el número de una tarjeta bancaria para cargar en la cuenta asociada a la misma el importe de la compra efectuada designan el n° de una tarjeta de la que no es titular ninguno de los acusados y es en la creencia de que todos los datos introducidos en la página web al hacer el pedido del reproductor de DVD son correctos por lo que la empresa R.F.S.L. procede a hacer la entrega de dicho aparato en el domicilio indicado al hacer el pedido*».

3.2. Medidas preventivas generales

Las posibilidades de fraude del que se pretende un beneficio económico y se determina un perjuicio patrimonial, inherentes a la mayoría de las operaciones económicas en las que interviene el consumidor, han encontrado —tal y como apuntamos— un magnífico marco de expansión en el medio internet. Ello se debe, entre otras razones, a la **gran vulnerabilidad que presentan muchos equipos de usuario**, desprovistos de las medidas de protección más elementales.

Para contrarrestar lo anterior, desde el punto de vista del usuario, resulta fundamental la adquisición de una **cultura de seguridad** en internet exactamente igual que la que se sigue en otros ámbitos de la vida cotidiana. Es preciso tomar las medidas de protección necesarias, fundamentalmente a través de un software adecuado frente a virus (programas capaces de reproducirse a sí mismos, infectando cualquier tipo de archivo ejecutable), troyanos (programas potencialmente peligrosos que se ocultan dentro de otros para evitar ser detectados, e instalarse de forma permanente en el sistema), programas espía *spyware* (que se instalan en el ordenador sin el conocimiento del usuario, para recopilar información del mismo, enviándola posteriormente al que controla dicha aplicación), etc. Los medios frente a todo lo anterior deben complementarse con las mismas medidas de

precaución y desconfianza que se adoptan en la vida diaria a la hora de custodiar claves, contraseñas o datos que puedan ser utilizados en el acceso a información personal, o aprovechados en actividades fraudulentas.

Así, como medidas generales de seguridad podrían, entre otras, adoptarse las siguientes: 1. Evitar en lo posible acceder en lugares públicos a cuentas de banca *on-line* y a cualesquiera otras páginas de comercio que impliquen nuestra identificación mediante claves. De hacerlo, siempre desconectarse y apagar el navegador, procurando que las *cookies* estén desactivadas y borrar el *cache*. 2. Actualizar el software (para tener así los últimos protocolos de seguridad) y antivirus/*antispyware*. 3. Comprobar que el sitio *web* desde el que se comercia transmite la información encriptada (protocolo de Seguridad) 4. Nunca acceder a peticiones de claves personales por mucho que la solicitud parezca cierta (proveniente del banco o empresa de *e-commerce* en cuestión). 5. Modificar las claves periódicamente. 6. No anotar las claves en lugares a los que pueda acceder cualquier otra persona y no transmitírselas a terceros. 7. Guardar copia de las operaciones de banca *on-line* o *e-commerce* realizadas. 8. Examinar en los accesos a la banca *on-line* la última fecha y ver si se corresponde con nuestro último acceso. 9. Revisar periódicamente las cuentas para ver si hay algún movimiento extraño y si lo hay reaccionar lo antes posible. 10. Suscripción a los sistemas que avisan con un mensaje al móvil cada vez que se realiza una operación, etc.

Como medidas específicas para protegerse del *phishing* sería precisa una correcta información, conociendo que las entidades financieras o asimiladas nunca piden por correo las claves de acceso; no acceder a la entidad *on-line* más que a través del vínculo de los «favoritos» o «bookmarks» o tecleando directamente la dirección web en el navegador; recordemos que las direcciones seguras siempre empiezan por https://. La protección específica frente al *spyware* pasa también por el empleo de herramientas tecnológicas capaces de evitar la entrada del mismo en los sistemas, bloqueándolo y eliminándolo eficazmente. Estos programas se encargan de monitorizar la actividad del sistema, para que en el caso de que haya algún archivo espía o similar sea detectado y neutralizado. Además de las posibles sustracciones por códigos maliciosos en el sistema, hay que tener en cuenta que en una conexión a Internet podemos ser víctimas de un ataque que puede conseguir acceso a nuestro ordenador. Para ello se vuelve imprescindible la instalación de un *firewall* personal (cortafuegos), que controle quién y cómo está intentando entrar en nuestro PC, consiguiendo de este modo evitar intrusiones dañinas.

3.3. Medidas o soluciones tecnológicas

Para hacer frente de un modo realista a la utilización delictiva de la Red conviene tener siempre presente que nos encontramos ante un medio en permanente evolución y por ello tremendamente dinámico, por lo que la mejor forma de hacer frente a las conductas fraudulentas es el recurso a una **investigación permanente en materia de seguridad y control**, que a buen seguro será más eficaz que la intervención del Derecho penal que si bien siempre llega tarde, en el caso de internet ese retraso se hace más evidente. En este sentido, sería conveniente que las compañías que transaccionan en la Red adoptasen las últimas medidas en materia de seguridad, siguiendo un esquema de reacción inmediata como el que utilizan las compañías antivirus.

En lo que respecta al comercio electrónico, resulta fundamental el desarrollo e implantación masiva de las distintas fórmulas dirigidas a obtener el máximo nivel de seguridad y entre ellas, de un modo especial, los certificados electrónicos. Para que la comunicación entre dos ordenadores sea confidencial se han desarrollado varios sistemas de cifrado de la información. El más usado actualmente, sobre todo en este tipo de comunicaciones (las compras en Internet), es el llamado *Secure Sockets Layer* (SSL). El SSL consiste, a grandes rasgos, en establecer unas claves entre el ordenador que se conecta y el servidor que se utiliza para que la información viaje cifrada entre los dos sistemas. De esta manera, si en algún punto de la comunicación hay algún elemento «espiando», la transacción será completamente ininteligible. Un certificado digital emitido por una de estas autoridades contiene la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el periodo de validez del certificado), todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la peculiaridad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra). Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación[16].

[16] Se puede hablar en este sentido de cuatro aspectos básicos de seguridad: autentificación, confidencialidad, integridad y el norepudio. La *autentificación* es el proceso de verificación formal de la identidad de las entidades participantes en una

Otros sistemas antifraude serían las tarjetas seguras de pago por internet o los Códigos de acceso de un sólo uso. Las primeras son tarjetas desechables destinadas a realizar pagos por internet, telefónicamente o por correo ordinario y que son recargables por un importe limitado. Los códigos de acceso de un solo uso, como su nombre indica, sólo tienen validez para una transacción, de manera que, una vez utilizado, queda anulado para usos posteriores. Se trata de un sistema compuesto por una aplicación en una tarjeta bancaria con un chip, un lector de tarjetas inteligentes y un sistema servidor. Con este sistema, el Código de un solo uso se genera en la tarjeta bancaria del cliente, que está protegida por los sistemas de seguridad que incluye el microprocesador de la propia tarjeta. También existen servicios ofrecidos por algunas compañías a las entidades que operan en la Red; son servicios de detección que tienen como objeto el descubrimiento temprano de ataques de *phishing*, incluso antes de que el mismo tenga lugar. Pueden detectar los incidentes en muchos casos desde su origen: en el momento de registro del dominio a utilizar, en

---

comunicación o intercambio de información. Existen varias formas de poder autentificarse: basada en claves, basada en direcciones y criptográfica. De estas tres posibilidades la más segura es la tercera, ya que en el caso de las dos primeras es posible que alguien intercepte la información enviada y pueda suplantar la identidad del emisor de información. Desde otro punto de vista se puede hablar de formas de autentificarse, como puede ser a través de la biometría (huellas digitales, retina del ojo, la voz (...)), por medio de *passwords* o claves, y por último utilizando un certificado digital. Se llama *autentificación fuerte* a la que utiliza al menos dos de las tres técnicas mencionadas en el párrafo anterior, siendo bastante frecuente el uso de la autentificación biométrica que, como se indicó antes, se basa en la identificación de personas por medio de algún atributo físico. La *confidencialidad* es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. La *integridad* consiste en que la información transmitida entre dos entidades no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales. Mediante una firma digital se codifican los mensajes a transferir, de forma que una función, denominada *hash*, calcula un resumen de dicho mensaje y se añade al mismo. La validación de la integridad del mensaje se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se añadió al final del mismo, cuando se calculo por primera vez antes de enviarlo. Mantener la integridad es importante para verificar que durante la transferencia por la Red de la información entre el sitio emisor y receptor nadie no autorizado ha modificado el mensaje. Los servicios de *norepudio* ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida. Con este aspecto conseguimos que una vez que alguien ha mandado un mensaje no pueda renegar de él, es decir, no pueda negar que es el autor del msmo. Es importante para el comercio electrónico, ya que garantiza la realización de las transacciones para las entidades participantes. Se aplica en ambos lados de la comunicación, tanto para no poder rechazar la autoría de un mensaje, como para negar su recepción. <http://www.portaley.com/comercio/seguridadce.shtml> [Consulta: 1 marzo 2007]

el lanzamiento del correo masivo por parte de quien pretende defraudar o desde que se activa un sitio web con la imagen de la entidad suplantada. Destaca también la creación de un sistema frente a los *spyware* que memorizan todo lo que se teclea enviando un reporte con esa información al defraudador *(keyloggers)*. El sistema consiste en concreto en el llamado «teclado virtual» o «en pantalla» *(Onscreen keyboard)* que es un programa que simula un teclado que se desplaza por la pantalla de forma que, mediante un ratón o un emulador de ratón, se puede escribir texto donde esté situado el punto de inserción o el texto resaltado[17].

4. Posibilidades de subsunción de las conductas fraudulentas ejecutadas a través de internet en los modelos típicos de estafa y estafa informática contenidos en el Código penal y propuesta de lege ferenda

Tratamos de analizar a continuación si todas las conductas fraudulentas antes descritas y otras que pudieran plantearse en el ámbito Internet, pueden ser subsumidas en alguno de los modelos de estafa recogidos en el Código Penal, ya sea la estafa común (art. 248.1) o en la llamada estafa informática (art. 248.2).

Los elementos caracterizadores del delito de *estafa común* son sobradamente conocidos por lo que nos limitamos a enunciarlos de modo escueto y atendiendo primordialmente a su configuración jurisprudencial. Así, el castigo penal por tal delito requiere la presencia de los siguientes: 1.º Un *engaño precedente o concurrente* concebido, con criterio amplio, atendiendo a la ilimitada variedad de supuestos que la vida real ofrece. Dicho engaño ha de ser «bastante», es decir, suficiente y proporcional para la consecución de los fines propuestos. Se tendrán en cuenta para valorar el engaño tanto las condiciones subjetivas del sujeto pasivo, como las objetivas que concurran en el caso. La maniobra defraudatoria ha de revestir apariencia de realidad y seriedad suficientes para engañar a personas de mediana perspicacia y diligencia. La idoneidad abstracta se complementa con la suficiencia en el específico supuesto contemplado. Dicho engaño puede ser implícito, explícito, activo u omisivo. 2.º Originación o producción de un *error esencial* en el sujeto pasivo desconocedor o con conoci-

[17] <http://www.aslan2.com/noticias/muestranoticia.asp?id=2248> [Consulta: 1 marzo 2007]

miento deformado e inexacto de la realidad, por causa del engaño, lo que le lleva a actuar bajo una falsa presuposición que parte de un motivo viciado y es causa de la subsiguiente disposición patrimonial. 3.º *Acto de disposición patrimonial*: la lesión del bien jurídico tutelado, el daño patrimonial, será producto de una actuación directa del propio afectado, consecuencia del error experimentado y, en definitiva del engaño, acto de disposición que ha de ser entendido, genéricamente, como cualquier comportamiento de la persona inducida a error, que arrastre o conlleve de forma directa la producción de un daño patrimonial en sí misma o en un tercero, no siendo necesario que concurra en la misma persona la condición de engañado y de perjudicado. Es en definitiva toda acción u omisión que implique un desplazamiento patrimonial, ya sea en forma de entrega, cesión o prestación de la cosa, derecho o servicio de que se trate o mero movimiento contable. No es necesario, en todo caso, que la disposición se efectúe por quien tiene la facultad jurídica de llevarla a cabo. 4.º El *perjuicio («en perjuicio»)* que se ocasiona como consecuencia de la transmisión patrimonial. El mismo puede afectar tanto a quien realiza la misma como a un tercero. El perjuicio típico habrá de ser tenido en cuenta para determinar la gravedad del delito. 5.º *Ánimo de lucro*, como elemento subjetivo del injusto, entendido como propósito por parte del infractor de obtención de una ventaja patrimonial correlativa. 6.º *Nexo causal* o relación de causalidad entre el engaño provocado y el perjuicio experimentado, ofreciéndose éste como resultado del primero. El engaño ha de motivar (producir) un error que induzca a realizar un acto de disposición que determine un perjuicio.

El criterio esencial para determinar en todo caso, y por tanto en los supuestos antes descritos, si es susceptible de aplicación el *delito de estafa común* pasará por comprobar si ha existido un *engaño (y consiguiente error)* ***que sufre una persona física como consecuencia de la trama engañosa elaborada por otra***. Es por tanto requisito *sine qua non* una relación/interlocución entre al menos dos personas: la que engaña y el engañado.

Pues bien, en base a ese criterio, entre los supuestos antes descritos, son susceptibles de subsunción en la «estafa común» los fraudes cometidos en operaciones de **comercio electrónico**, tanto si el que defrauda es el comprador como el que oferta el producto. En el primer caso se produce la adquisición de un producto a través de internet por parte de un sujeto (el engañado) al que finalmente no se le envía o, aún enviándoselo, resulta ser defectuoso o distinto de lo pactado, aspecto conocido y predispuesto por el vendedor (el que engaña). También, en principio, habrá estafa común en aquellos supuestos en que es el comprador el que elude, de algún modo, pagar al

vendedor (el engañado) el precio pactado, quedándose sin embargo con el bien recibido.

También son susceptibles de ser castigados a través del delito de estafa común los supuestos de fraude cometidos a través de ***phishing***; recordemos como en este caso, un sujeto (el que engaña) hace llegar un mensaje a las posibles víctimas, consiguiendo que algunas de ellas (engañadas) hagan constar datos o claves personales, que serán posteriormente utilizados por el defraudador para realizar una transferencia en favor propio o de un tercero.

La misma situación se plantea con los ***mails*** **fraudulentos** en los que el remitente (el que engaña) solicita de la victima y esta ejecuta alguna actividad (disposición) que redundará en beneficio del primero y en perjuicio de si misma (engañada). Surgen aquí, sin embargo, dudas sobre la efectiva presencia de la «disposición patrimonial», pues la misma no la realiza «el propio afectado», lo que hace conveniente relegar también este supuesto al tipo de la estafa informática.

En todos los casos expuestos —salvo la última excepción comentada— no existen mayores dificultades para su subsunción en el delito de estafa común recogido en el art. 248.1 al margen, claro está, de la necesaria presencia del resto de elementos típicos. Sin embargo, de entre las conductas antes descritas, existen otras cuya dinámica comisiva no encaja en esta modalidad típica, básicamente *por estar ausentes los elementos de engaño y error que debe sufrir la víctima como consecuencia de una trama fraudulenta*. En efecto, recordemos que no pueden ser castigadas a través del delito de estafa común todas aquellas conductas en las que falta un sujeto persona física *que sufre el engaño*. Son supuestos en los que sólo interviene el primer sujeto (el defraudador) sin que exista otro al que se dirija la maniobra engañosa. Aquí quedarán ubicados, de entre los supuestos antes planteados, los casos de fraudes a través de algunos tipos de *spyware*; recordemos que se trata de archivos que, una vez introducidos en el ordenador sin que la víctima sea consciente de ello, envían a través de la Red las claves de acceso a diferentes servicios informáticos y entre ellos las de banca *on-line*, con las cuales el defraudador puede realizar una disposición fraudulenta a su favor o en favor de un tercero. Lo mismo puede decirse de aquellos casos en los que el defraudador, mediante el acceso al sistema, consigue hacer desaparecer o disminuir deudas propias o ajenas. Obsérvese que en tales supuestos (y en todos los que posibiliten la obtención de las claves de acceso sin intervención de su titular) no hay ningún mensaje dirigido a la víctima para que esta haga algo (no hay engaño ni error). Situación parecida se plantea en

los fraudes cometidos a través de los *dialers*, que se instalan sin el conocimiento de la víctima, determinando conexiones telefónicas de alto coste que son posteriormente facturadas[18].

Precisamente debido a la insuficiencia de la estafa común para resolver algunos supuestos en los que está ausente el engaño y error definitorios de este delito, el legislador de 1995 creó un nuevo modelo de estafa, la llamada *estafa informática*. La misma aparece configurada en el art. 248.2 CP con el siguiente tenor literal: «*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*».

Tal y como apuntamos, la previsión de esta nueva modalidad tiene **su razón de ser** en la **insuficiencia del modelo clásico de estafa** para hacer frente a los supuestos de manipulaciones informáticas, en los que *no están presentes ni el engaño ni el error* que, como es sabido, son elementos esenciales de la estafa común[19]; todo ello bajo la idea de que actuar sobre ordenadores o terminales no es una forma de engaño porque «a las máquinas no se les puede engañar»[20]. El au-

---

[18] Un supuesto de instalación de un *dialer* con conocimiento de la víctima, circunstancia que determinó en consecuencia la absolución de los imputados, lo encontramos en la Sentencia del Juzgado de Primera Instancia e Instrucción núm.1 de Toledo de 22 de abril de 2003: «*D. A.F.R.R. en el acto del juicio admite que fue su hijo quien se conecto a una línea erótica, desconociendo si llego a aceptar alguna oferta de conexión a Internet, admite igualmente que cuando se conectaba a esa línea se lo advertía. (...) debe dictarse una sentencia absolutoria (...)*». También absolutoria por las mismas razones es la Sentencia del Juzgado de lo Penal núm. 3 de Valladolid de 24 de enero de 2005: «*(...) No obstante su accionamiento no tenía efecto alguno, a no ser que, previamente, se hubiese marcado una casilla de verificación, situada inmediatamente debajo, cuya leyenda era: «Soy mayor de edad y acepto la tarifa de 0'91 euros/min + establecimiento llamada 0'09 euros + IVA 16%*».

[19] *Vid.*, ROMEO CASABONA C. R., «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», en *Poder Judicial*, 2ª época, número 31, septiembre de 1993, p. 180 y ss. GUTIERREZ FRANCÉS M. L., «Delincuencia económica e informática en el Nuevo Código Penal», en *Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial*, XI, 1996, p. 247 y ss. La misma, en *Fraude informático y estafa: (aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos)*, Ministerio de Justicia, Madrid, 1991. GONZÁLEZ RUS J. J., «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», en *RECPC*, 1-14, 1999, <http://criminet.ugr.es/recpc/recpc_01-14.html> [Consulta: 1 marzo 2007]. ORTS BERENGUER E.-ROIG TORRES M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001, p. 62. MATA Y MARTÍN R., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, p. 41.

[20] Antes de la regulación penal de la estafa informática, la jurisprudencia intentó acomodar esas conductas a las figuras ya existentes; sin embargo dicha opción resultaba prácticamente inviable. Esta insuficiencia se puso de manifiesto por ejemplo

tor del delito no ha utilizado ninguna treta ni artimaña para viciar la voluntad de la víctima, puesto que la acción empieza en el ordenador, pero no tiene a ninguna otra persona física como destinatario. Sin embargo, en los supuestos subsumibles en la estafa informática *sí existe el ánimo de lucro*, puesto que quien defrauda actúa guiado por ese afán de enriquecerse económicamente, *y el perjuicio a tercero*, ya que se produce un detrimento económico al patrimonio de otra persona. Esta idea puede verse claramente explicada en la STS de 21 de diciembre de 2004 (RJ 2004/8252): «*El tipo penal del art. 248.2 CP tiene la función de cubrir un ámbito al que no alcanzaba la definición de la estafa introducida en la reforma de 1983. La nueva figura tiene la finalidad de proteger el patrimonio contra acciones que no responden al esquema típico del art. 248.1 CP, pues no se dirigen contra un sujeto que pueda ser inducido a error. En efecto, los aparatos electrónicos no tienen errores como los exigidos por el tipo tradicional de la estafa, es decir, en el sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio, sin error*». A ello añade la STS de 20 de noviembre de 2001 (RJ 2002\805) que «*el engaño, propio de la relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante*».

Debe advertirse, sin embargo, que el tipo de la estafa informática no nació en absoluto con objeto de resolver situaciones fraudulentas ejecutadas a través de internet, pues recuérdese que la introducción del mismo en el Código penal se produce en un momento en el que aún no se había producido un desarrollo significativo del uso de la Red en nuestro país. Realmente el principal objetivo perseguido con su tipificación era el de sancionar situaciones fraudulentas planteadas en entidades bancarias o terminales de pago (TPV) en las que algún empleado o tercero, operando sobre las mismas, realiza transferencias a su favor o en favor de tercero. De hecho, en los años de vigencia del tipo de la llamada estafa informática, ésta ha sido utilizada fundamentalmente para castigar operaciones fraudulentas ejecutadas con tarjetas de crédito/débito en cajeros automáticos[21]. Hasta su in-

---

en la STS de 19 de abril de 1991 (RJ 1991\2813), en la que se enjuició la conducta de un empleado de banca que manipuló las cuentas corrientes de varios clientes a través del ordenador y se embolsó más de 3.000.000 ptas. (18.030 euros). El tribunal consideró —correctamente— que no había estafa, ya que no se produjo el engaño en las victimas que les llevara al error necesario que, a su vez, determinara la realización de la disposición patrimonial a favor del autor del delito.

[21] Si en vez de usar la tarjeta en el cajero, la misma se entrega a un tercero para efectuar un pago estaremos ante un *delito de estafa común*, pues se engaña, en cuanto a la identidad, a una persona (la que recibe la tarjeta): así, por ejemplo, STS de 8 de

troducción, este tipo de operaciones en la práctica eran penalmente sancionadas, de modo muy discutible, a través de la figura del *robo con fuerza en las cosas por uso de llave falsa*, en el que la tarjeta recibía tal consideración[22].

Así, puede verse dicha transición en la explicación contenida en la Sentencia del Juzgado de Barcelona de 8 de mayo de 2003 (JUR 2003\87807): «*Pero es que además, a tales críticas expuestas por la doctrina más reciente y la jurisprudencia menor citada de los últimos años se aúnan los nuevos criterios y argumentos jurisprudenciales sentados a partir de la Sentencia del Tribunal Supremo de 201101 (RJ 2002, 805) en referencia al uso ilícito de tarjetas de crédito o débito ajenas en Terminales Punto de Venta (TPV), en su consideración de tales acciones como subsumibles en la figura del artículo 248.2 del Código Penal, y que son perfectamente extrapolables al presente supuesto de acciones de obtención de dinero en metálico de cajeros automáticos mediante el uso ilícito de tarjetas de crédito o débito ajenas (...)*». «*(...) que no engaño propiamente dicho como operación vincular entre personas físicas pues no hay persona física engañada, también se exterioriza en la simulación o suposición de quien realiza el acto mercantil base de la operación de cargo es el titular de la tarjeta (...)*». La misma solución por ejemplo, en la STS de 20 de noviembre de 2001 (RJ 2002\805), en la SAP Navarra de 13 de mayo de 2002 (JUR 2002\178058), o en la más reciente SAP Baleares de 14 de abril de 2005 (JUR 2005\106316), entre otras.

Las sentencias citadas (referidas al uso ilícito de tarjetas en cajeros) subsumen tales conductas en el concepto de «**manipulación informática**» o incluso en algún caso en el de «**otro artificio semejante**». Sin embargo, ninguna de ellas explica convenientemente donde está dicha manipulación o artificio[23]. En puridad, a mi juicio, en tales casos

julio de 2002 (RJ 2002\8939) en la que los sujetos condenados habían copiado el contenido (datos codificados grabados electrónicamente) de las bandas magnéticas originales de varias tarjetas de crédito, con ocasión de ser utilizadas por sus legítimos propietarios en un determinado establecimiento comercial, utilizando para ello un aparato grabador fabricado al efecto. Posteriormente fueron usadas en un comercio para pagar determinados bienes, siendo ahí donde aparece el engaño y error de la estafa común (entregada a una persona física que sufre el error respecto a la verdadera identidad de quien le presenta la tarjeta).

[22] Aún, en contra de la jurisprudencia del Tribunal Supremo, encontramos alguna sentencia que resuelve castigando como robo con fuerza en las cosas por uso de llave falsa: SAP Sevilla de 10 de marzo de 2004: «*la extracción de dinero de cajero automático mediante la tarjeta de crédito previamente sustraída a su legítimo titular constituye sin duda el delito de robo con fuerza en las cosas de los artículos 237, 238.4.º, 239.3.º y 240 CP*».

[23] La STS de 20 de noviembre de 2001 (RJ 2002\805) sí hace un intento, a mi juicio escasamente satisfactorio, de explicar la subsunción en el concepto «artificio semejante»: «*Cuando la conducta que desapodera a otro de forma no consentida de su*

no existe ninguna manipulación de carácter informático (pues se introducen datos ciertos). Lo que, en mi opinión, realmente se presenta es una **utilización ilegitima** de las tarjetas y sus claves[24] (en el caso de uso de tarjetas en cajeros) y únicamente de sus claves (en el caso de fraudes cometidos a través de internet que determinan la sustracción de sus claves sin intervención consciente de su titular)[25].

Veamos a continuación si pueden ser subsumibles en dicho concepto (manipulación informática o artificio semejante) todos aquellos supuestos, a los que ya nos referimos, que no encajan en la estructura de la estafa común (engaño-error-disposición patrimonial-perjuicio). Recordemos que se trata de conductas en las que falta un sujeto persona física que sufre el engaño o al que se dirija la maniobra engañosa. Se incluirían en ese modelo los casos de fraudes a través de algunos tipos de *spyware* que envían a través de la Red las claves de acceso a diferentes servicios y también los fraudes cometidos a través de los *dialers* de conexión telefónica, que se instalan sin el conocimiento y consentimiento de la víctima, produciendo ambas un perjuicio económico.

---

patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del Código Penal. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que éste signifique artimaña, doblez, enredo o truco. La conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado». Según MATA Y MARTÍN R. M., «Algunas consideraciones sobre informática y Derecho penal. El caso de la estafa informática», en *Documentos Penales y Criminológicos*, vol. 1, 2001, p. 48, la *manipulación informática* determina una actuación sobre un sistema informático de manera que este altere el resultado al que habría de conducir el normal procesamiento automático de datos. La misma puede tener lugar en la elaboración del programa, en la configuración del mismo o, una vez elaborado, en los datos que se introducen en su ejecución.

[24] Distintos son los casos en los que se produce una auténtica manipulación en la banda magnética en la tarjeta o en el propio cajero: por ejemplo, SAN de 10 de marzo de 2001 (JUR 2001\170088) referida a un supuesto de pagos con tarjetas de crédito, falsificadas mediante la introducción en su banda magnética de datos pertenecientes a un titular distinto.

[25] El proyecto de reforma del código penal, actualmente en tramitación parlamentaria (Proyecto de Ley —121/000119— Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal) pretende resolver las dudas existentes al prever como una forma más de estafa el uso de tarjetas de crédito o débito o de sus datos obrantes en ellos para realizar operaciones de cualquier clase en perjuicio de su titular o de un tercero: «*Art. 248: (...) 2. También se consideran reos de estafa (...) c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero*».

Para ello es preciso determinar previamente que ha de entenderse por **manipulación informática o artificio semejante**. Pues bien, según el concepto más extendido derivado fundamentalmente de la interpretación jurisprudencial [STS de 20 de noviembre de 2001 (RJ 2002\805) y STS de 26 de junio de 2006 (RJ 2006\4925)] lo relevante será que la máquina, informática o mecánica, *actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos*. «Alteración de elementos físicos y de programación» e «introducción de datos falsos» serán pues los elementos necesarios para poder afirmar la presencia de tal modalidad de conducta[26].

Pues bien, el concepto de «*manipulación informática o artificio semejante*», al menos así entendido, va a dificultar la subsunción en el tipo de los supuestos de **obtención y posterior uso de las claves a través de *spyware* u otro método que no implique la intervención de la víctima**[27]. No parece claro dónde está la manipulación informática en tales supuestos, pareciendo más bien que se ha forzado el sentido de las palabras más allá de lo lícitamente admisible. No se trata de alteración de elementos físicos ni de programación ni introducción de datos falsos. Quien ha obtenido las claves (auténticas) y las utiliza desde su propio ordenador, para realizar una transferencia a su favor o de un tercero (cambio de titularidad de los activos) a través de la Red, no ha alterado elemento físico o de programación alguno.

Es cierto que en algún caso, el Tribunal Supremo se ha visto obligado a «simplificar» la definición de estafa informática para resolver

[26] El resto de elementos típicos del delito de estafa informática no plantean especial dificultad; así, la misma exige que los autores «*consigan la transferencia no consentida de cualquier activo patrimonial*», siendo suficiente para ello el cambio fáctico de adscripción del elemento patrimonial; vid. PÉREZ MANZANO M., en *Compendio de Derecho penal. Parte especial*, vol. II, Ceura, Madrid, 1998, p. 456. Considera J. A. CHOCLÁN MONTALVO («Fraude informático y estafa por computación», *loc. cit.*, p. 338) que la obtención de un servicio sin abono de su importe es equivalente a la transferencia de un activo patrimonial. La referencia a los *activos patrimoniales* tiene como clara finalidad precisamente englobar valores patrimoniales que no tienen correspondencia con un objeto material; vid. MATA Y MARTÍN R. M., «Algunas consideraciones sobre informática», *op. cit.*, p. 109. El precepto exige además otros dos requisitos de la estafa común *(«con ánimo de lucro y en perjuicio de tercero»)*, cuyo significado es sobradamente conocido.

[27] Defiende, A. GALÁN MUÑOZ (*El fraude y la estafa mediante sistemas informáticos*, Tirant lo Blanch, Valencia, 2005, p. 559 y ss.) un concepto muy amplio de «manipulación informática» que permitiría subsumir en dicha figura cualquier conducta realizada mediante la utilización de sistemas informáticos idónea para conseguir una transferencia no consentida de activos patrimoniales; deja de este modo carente de todo contenido la segunda modalidad típica *(«otro artificio semejante»)*.

un caso concreto en el que no eran útiles los conceptos descritos; así, la STS de 21 de diciembre de 2004 (RJ 2004\8252), según la cual para colmar la acción típica de la estafa informática será suficiente la presencia de dos requisitos: el primero, que el autor carezca de autorización para usar el medio informático y el segundo que produzca «efectos semejantes a la estafa común»[28]. Con ello consigue condenar por estafa informática el supuesto enjuiciado, referido a la manipulación por terceros del terminal de venta situado en un establecimiento comercial, realizando operaciones de abono en favor del defraudador. Sin embargo obsérvese que, como apuntamos, *ni siquiera esa interpretación amplia podría determinar la condena por estafa informática en los supuestos descritos de uso de spyware y posterior utilización de las claves*, pues el defraudador no carecerá de autorización para usar *el medio informático* en el momento de realizar la transferencia ilícita, ya que normalmente actuará (introduciendo las claves sustraídas) sobre un equipo propio de uso legítimo.

Idénticos problemas se suscitan con las nociones elaboradas por diversas Audiencias Provinciales; así, por ejemplo, de acuerdo con la SAP Málaga de 4 de noviembre de 2002 (JUR 2003\90990) «*el engaño, propio de la relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante, en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos*». Sin embargo, en el caso por nosotros planteado (introducción de claves auténticas inicialmente sustraídas) en ningún momento se alteran elementos físicos del sistema informático ni su programación, como tampoco se in-

[28] STS de 21 de diciembre de 2004 (RJ 2004\8252): «*De cualquier manera, el art. 268 CP no es aplicable al caso, dado que la acción, que la Audiencia debería haber subsumido correctamente en el núm. 2 del art. 248 CP, (...) fue realizada empleando instrumentos informáticos que se encontraban en el ámbito de dominio de éstos y que permitían, evidentemente, efectuar disposiciones sobre el patrimonio del mismo. Dado lo claramente justificado de la pena, el recurrente no ha impugnado la subsunción realizada por la Audiencia. Lo importante es, ante todo, la realización de las acciones constitutivas de un artificio semejante a una manipulación informática. En efecto, al texto del art. 248.2 CP considera aplicable la pena de la estafa cuando el autor se ha valido de «alguna manipulación informática» o de algún «artificio semejante». La cuestión de cuáles son los artificios semejantes debe ser determinada por la aptitud del medio informático empleado para producir el daño patrimonial. En este sentido es equivalente, a los efectos del contenido de la ilicitud, que el autor modifique materialmente el programa informático indebidamente o que lo utilice sin la debida autorización o en forma contraria al deber. En el presente caso, por lo tanto, el recurrente carecía de autorización para utilizar el medio informático y, además, produjo efectos semejantes a la misma, sobre el patrimonio del Banco*».

troducen datos falsos (se hacen constar, insistimos, las claves auténticas, a través de una suplantación del titular de las mismas).

Pero es que además, de un modo más contundente, no parece que sea posible mantener con un mínimo rigor que en el supuesto fraudulento antes enunciado referido a los ***dialers*** podamos estar ante alguna forma de «manipulación informática o artificio semejante». Recordemos que son programas de marcado telefónico que se pueden autoinstalar sin conocimiento del sujeto y que establecen una conexión de acceso telefónico a redes mediante un número de tarificación adicional, lo que reporta un beneficio al titular de la línea telefónica. En este caso, ya ni siquiera nos queda el acto de suplantación de personalidad a donde reconducir (de modo muy discutible) la «manipulación».

En ocasiones, las graves deficiencias de configuración en la estafa informática, y la consideración judicial de que la conducta examinada merece respuesta penal, han determinado incluso que el tribunal opte —insólitamente— por aplicar la estafa común, todo ello en neta contradicción con la teoría —ampliamente consolidada— según la cual, en tal supuesto no cabe apreciar la estafa común, pues *a las máquinas no se les puede engañar*[29].

En realidad, los casos de utilización ilegítima de las claves en el ámbito internet (conseguidas a través de *spyware* u otro medio, sin que intervenga su titular) que permiten al sujeto hacerse con el patrimonio de la víctima poseen una dinámica comisiva compuesta por dos fases: **a)** La sustracción inmaterial de las claves. **b)** Su uso ilícito, suplantando la personalidad del verdadero titular (además de la transferencia patrimonial, beneficio y perjuicio).

---

[29] Por ejemplo, la SAP Navarra de 27 de febrero de 2004 (JUR 2004\112086) en la que se enjuicia un fraude consistente en la selección en un cajero de la opción de recarga de móviles, solicitándola por el importe determinado, estando el teléfono que se va a cargar sin nada de saldo y preparado un mensaje para enviar. El operador de Telefónica, autoriza la carga y, antes de que aparezca en la pantalla del cajero que la operación se deniega por falta de fondos, se envía el mensaje preparado, para hacer un gasto en el saldo ya cargado en el importe solicitado, por lo que al anular inmediatamente Telefónica la carga, esta anulación no se hace efectiva, al haber un saldo inferior por el mensaje enviado. Pues bien, la Audiencia excluye la aplicación del delito de estafa informática «*por estar ausente la manipulación informática u otro artificio semejante*». Sin embargo, y de modo sorprendente acude a la estafa común, pese a que es evidente la ausencia de error y engaño en base al citado criterio del Tribunal Supremo: «*Es por ello a juicio de la Sala, que si alguna duda pudiera caber respecto de la consideración de los hechos como una estafa «informática», por la ausencia de acción manipuladora propia del menor, la concurrencia de todos los requisitos para la exigencia de responsabilidad penal por el delito de estafa genérica no puede ofrecer ninguna duda, pues se utiliza engaño, que genera un error en el sistema informático, desencadenante del acto de disposición*».

a) La sustracción inicial de las claves (mediante *spyware* u otros medios) y antes de que se lleguen a utilizar sería un acto previo que no es relevante por si solo desde el punto de vista penal patrimonial[30], siguiendo para ello el criterio establecido jurisprudencialmente en los casos de sustracción de las claves de una tarjeta para posteriormente ser utilizadas en un cajero o comercio. Así, por ejemplo SAP Sevilla de 10 de marzo de 2004 (JUR 2004\126830) referida a la extracción de dinero de cajero automático mediante la tarjeta de crédito, previamente sustraída a su legítimo titular con sus claves y en la que se determina que la sustracción por ese procedimiento de las claves (dígitos alfanuméricos) «*no es reconducible a ningún delito patrimonial*». Si dicha conducta de sustracción de claves u otros elementos no determina finalmente un objetivo lesivo patrimonial debe, sin embargo, examinarse si la misma ha podido constituir autónomamente uno de los delitos contra la intimidad contenidos en el art. 197 y ss., con la dificultad —cuando no imposibilidad— de incluir ese tipo de datos en el concepto de intimidad personal.

b) El uso o utilización ilícita de las claves suplantando la personalidad del verdadero titular. Ya hemos visto que esta conducta no puede ser subsumida en la estafa común por la ausencia de engaño sobre un tercero. A la vez, comprobamos que su subsunción en los conceptos «manipulación informática» o «artificio semejante» resulta enormemente compleja, pudiendo constituir un auténtico fraude de etiquetas, pues no hay ninguna manipulación, no hay ninguna alteración. Lo que se produce es una suplantación respecto al verdadero titular, ya que el que introduce determinadas claves afirma con ese acto ser determinada persona, pues son claves personales que identifican únicamente al sujeto titular de las mismas. Se manipula la realidad a través de medios informáticos (son el mero canal de comunicación). No hay alteración alguna del sistema o software que lo soporta. Aunque dicha conducta, eventualmente, pudiera ser reconducida a formas falsarias, quedaría totalmente desprotegido el aspecto lesivo patrimonial.

Por todo ello, creemos que el modelo vigente de estafa informática debería ser sustituido por uno nuevo que pueda hacer frente sin tensiones a todos los supuestos analizados. El mismo se debe caracterizar por el castigo de ***la ejecución, con ánimo de lucro, de operaciones informáticas no autorizadas perjudiciales para el patri-***

[30] El proyecto de reforma del código penal, actualmente en tramitación parlamentaria (Proyecto de Ley —121/000119— Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal), prevé la introducción de una modalidad delictiva que castiga ese tipo de conductas.

monio de otro. El elemento nuclear y la clave de dicha propuesta es doble; en primer lugar, la ejecución de ***operaciones*** (y no manipulaciones) informáticas, expresión de carácter más genérico, que permite subsumir todos los casos expuestos y, en segundo lugar, la referencia a la ***falta de autorización*** que constituye el elemento clave definidor de este tipo de conductas, igual que lo es el engaño en la estafa común. Esa presencia de una operación informática no autorizada es lo que caracteriza también al supuesto comisivo basado en *dialers*, los cuales determinan una conexión a la Red (operación informática) no autorizada (en esas condiciones).

La dinámica comisiva propia de muchos de las conductas descritas, especialmente las ventas fraudulentas, presentan las características necesarias para la apreciación de la figura del delito continuado; la reiteración del fraude (pluralidad de hechos ontológicamente diferenciables), presencia de un dolo unitario, unidad de precepto penal violado, homogeneidad en el *modus operandi*, y, finalmente, que las diversas acciones se hayan desenvuelto en el mismo o aproximado entorno espacio-temporal.

5. Precursores: software necesario para cometer los fraudes

Con el ánimo de intensificar la protección, la reforma 15/2003 de modificación del Código Penal añadió un apartado 3 al artículo 248, quedando redactado como sigue: «*La misma pena* (nítida vulneración del principio de proporcionalidad) *se aplicará a los que fabricaren, introdujeren, poseyeren o* ***facilitaren programas de ordenador específicamente destinados a la comisión de las estafas*** *previstas en este artículo*»[31].

El objetivo de este precepto es por tanto anticipar la intervención penal a momentos previos a la realización efectiva del fraude. De este modo, se castiga determinadas conductas ejecutadas sobre los precursores; esto es sobre aquellos elementos necesarios para come-

[31] El proyecto de reforma del código penal, actualmente en tramitación parlamentaria (Proyecto de Ley —121/000119— Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal), no se limita a extender la pena prevista para el delito de estafa, tal y como hace la redacción vigente, sino que directamente considera —de forma incomprensible— a sus autores reos de estafa: «*Art. 248 (...) 2. También se consideran reos de estafa: (...) b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*».

ter el fraude, que en este caso es básicamente el software usado para la estafa. Se trata en concreto de programas que facilitan o resultan imprescindibles para la comisión de las conductas fraudulentas analizadas. Es por ejemplo el caso de los *keyloggers*, que son aplicaciones que tienen como objetivo capturar las pulsaciones sobre el teclado. Las mismas pueden enviar información clave (*logins*, *passwords*, números de cuentas o de tarjetas de crédito, etc.) a quien pretende cometer el fraude. Otro ejemplo son los *sniffers*, que pueden ser utilizados para capturar los datos que son transmitidos en la red o los crackeadores de contraseñas, esto es programas que prueban diferentes *passwords*, uno tras otro, hasta dar con el correcto.

Las conductas típicas que recaen sobre los precursores son casi todas las imaginables, castigándose de este modo, no sólo al que los fabrique (programe), sino también a quienes los introdujeren o facilitaren, e incluso a quienes meramente los poseyeren. En todo caso, cualquiera de estas conductas debe ir acompañada para su punición, además del ánimo de lucro del tipo básico, de un elemento subjetivo finalístico consistente en actuar con el ánimo de cometer la estafa, pues dicho requisito (*específicamente destinados a la comisión de las estafas*) debe entenderse referido conjuntamente tanto al tipo de software como a la intencionalidad del autor. Debe recordarse en tal sentido que muchos de los programas con potencialidad fraudulenta pueden tener también un uso lícito.