
Revista
Enero 2012
29
tirant lo blanch

Revista Penal

Número 29

Sumario

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, Pablo Olavide de Sevilla y la Cátedra de Derechos Humanos Manuel de Lardizábal.

www.revistapenal.com

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL:
ISSN.: 1138-9168
IMPRIME: Guada Impresores, S.L.
MAQUETA: PMc Media

Nuevas formas de criminalidad patrimonial a través de internet*
New forms of criminality against property throug internet

Fátima Flores Mendoza

Profesora Titular de Derecho Penal
Departamento de Disciplinas Jurídicas Básicas
Universidad de La Laguna
fflores@ull.es

Revista Penal, n.º 29.— Enero 2012

***RESUMEN**: Este trabajo se ocupa de la respuesta penal a una nueva forma de criminalidad en el ámbito de la banca electrónica, denominada phishing, y consistente en la utilización no consentida de las claves de acceso a cuentas bancarias electrónicas ajenas para realizar transferencias bancarias en perjuicio de terceros a través de la red.*

***PALABRAS CLAVE**: phishing, fraude informático, cibercrimen*

***SUMMARY:** This article is focused in the criminal answer to a new form of criminality at the on line bank, named phishing. It consists of the illegal use of the password to the on line bank accounts to transfer money through the electronic net*

***KEY WORDS**: phishing, computer fraud, cibercrime*

I

En los últimos años el Derecho Penal se enfrenta a una compleja realidad como es Internet, que ha roto con los modelos tradicionales de comunicación e información. Las características exclusivas de Internet −amplitud y diversidad de contenidos, automatismo, interactividad, multiubicación, uso generalizado, alcance global o internacional y descentralización− representan su gran potencial, pero también el origen de la vulnerabilidad del sistema, convirtiéndolo asimismo en un poderosísimo instrumento técnico al servicio del crimen. Por un lado, por las dificultades para el control de las comunicaciones e información que circula por la red: por las colosales dimensiones del número de usuarios y de la información, las frecuencias de acceso y su carácter descentralizado. Por otro lado, por su potencialidad multiplicadora para ampliar sus efectos debido, entre otras características a su alcance global e internacional. Y, finalmente, por las dificultades que presentan el descubrimiento y persecución de los delitos cometidos a través de ella: gracias a la posibilidad de acceder de forma anónima o a través de identidad falsa, de acceder a la red desde cualquier terminal o servidor del ciberespacio en cualquier momento y cambiar unos y otros con

* Este trabajo se realiza en el marco del proyecto de investigación DER2008-00954/JURI "Delincuencia económica. Nuevos instrumentos jurídicos y tecnológicos", concedido por el Ministerio de Ciencia y Tecnología.

total facilidad, así como de ocultar la comisión del delito[1].

Entre los delitos más frecuentes cometidos a través de Internet se encuentran los denominados delitos informáticos: accesos no autorizados a información ajena o interceptación de las comunicaciones (espionaje); ataques contra redes y sistemas informáticos, por ejemplo, alteración, obstrucción o inutilización de datos o sistemas (sabotaje); atentados contra los derechos de autor y derechos afines, entre los que se encuentran los supuestos de reproducción no consentida de creaciones intelectuales o industriales (piratería), etc. Pero también está sirviendo de medio técnico para la comisión de otros delitos relativos a la pornografía infantil, incitación a la xenofobia, apología del terrorismo (ciberterrorismo) a través de la difusión de dichos contenidos ilícitos, así como de otros convencionales como atentados contra el honor, la libertad (ciberacoso) el patrimonio y orden socioeconómico, la seguridad del Estado, etc.[2].

Entre los atentados al patrimonio mediante el uso de las nuevas tecnologías encontramos junto a los, ya mencionados, de sabotaje y piratería, las defraudaciones, que son numerosas y de diversos tipos[3]. Los más simples utilizan Internet para el envío de correos masivos con los que engañar a sus víctimas ofreciéndoles premios, regalos, productos, trabajo, servicios, previo desembolso de una cantidad económica y que constituyen estafas comunes. También son frecuentes en las operaciones de subastas o comercio electrónico, tanto por parte del vendedor −que entrega un producto que no se corresponde con el ofertado, o que simplemente no envía tras haber recibido el pago anticipado− como del comprador, que no abona el producto. Otro de los supuestos consiste en la descarga no consentida en el sistema informático del usuario de Internet de programas de conexión telefónica a redes con tarifación adicional de altísimo coste (*dialer*).

Todos estos ataques se han visto favorecidos, entre otros factores, por el desconcierto inicial, la limitada experiencia y escaso conocimiento de usuarios y administradores, la débil percepción de riesgo de algunos usuarios, pero también por la falta de denuncia de muchos de estos atentados con el propósito de evitar la publicidad negativa y ocultar la vulnerabilidad del sistema[4].

En este trabajo me centraré en la respuesta que ofrece nuestro Código Penal a un nuevo supuesto de atentado contra el patrimonio que se lleva realizando en nuestro país desde hace unos años en el ámbito de la banca en línea y que consiste en la utilización ilícita de claves de acceso y firma electrónica de cuentas bancarias para realizar traspasos patrimoniales en perjuicio de terceros a través de la red.

La compleja ejecución de estas conductas se desarrolla en tres fases, realizadas por sujetos de diferentes nacionalidades, previamente concertados y organizados, y actuando en diferentes estados, lo que dificulta su persecución[5]. La primera tiene por objetivo la obtención ilícita de datos confidenciales para el control de las cuentas bancarias (claves secretas de acceso y firma electrónica) de las víctimas a través de Internet y mediante diversas modalidades. Entre las más frecuentes se encuentra el *phishing* o pesca de datos. Esta modalidad consiste en el envío masivo e indiscriminado de correos electrónicos a usuarios de la red solicitando las claves y números secretos de cuentas bancarias, tarjetas, etc., aparentando proceder de bancos, cajas de ahorro u organismos oficiales, y alegando motivos de seguridad, mantenimiento, mejora del servicio, etc.[6/7]. Una modalidad similar es la del *pharming*. Aquí se utiliza la red para

1 V. C. M. ROMEO CASABONA, «De los delitos informáticos al Cibercrimen» en *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*: C. M. Romeo Casabona (Coord.), Comares, Granada, 2006, pp. 2 y ss.

2 V. L. PICOTTI, «Internet y Derecho Penal: ¿Un empujón únicamente tecnológico a la armonización internacional?» en *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*: C. M. Romeo Casabona (Coord.), Comares, Granada, 2006, p. 362.

3 Sobre ellas v. más ampliamente los trabajos de J. G. FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, CCC, 2007 y P. FARALDO CABANA, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Tirant lo Blanch, Valencia, 2009.

4 Así lo han puesto de manifiesto FARALDO CABANA, *Las nuevas tecnologías*, 23 y FERNÁNDEZ TERUELO, *Cibercrimen*, p. 27.

5 Ampliamente sobre la ejecución de estos ataques al patrimonio en nuestro país v. Auto AP Barcelona de 23 de octubre de 2009. V. también el trabajo de C. F. STUCKENBERG, «Zur Strafbarketi von "Phishing"» en *ZStW* (118), 2006, pp. 878 y ss.

6 El *phishing* deriva del término *fishing* (pesca), puesto que la técnica consiste en pescar a los incautos internautas con el "cebo" de los correos electrónicos. En el lenguaje de la red la "f" se sustituye por "ph". Sobre este punto v. STUCKENBERG, ult. luc. cit. Más ampliamente sobre esta modalidad, v. FERNÁNDEZ TERUELO, *Cibercrimen*, pp. 29 y s.; E. VELASCO NÚÑEZ, «Estafa informática y banda organizada. *Phishing, pharming, smishing* y muleros» en *La Ley Penal (LLP)*, 2008, p. 21; EL MISMO, «Fraudes informáticos en la red: del *phishing* al *pharming*» en *La Ley Penal*, 2007, pp. 57 y s.

acceder al sistema informático de un tercero y cambiar las direcciones electrónicas contenidas en el servidor DNS (*Domain Name Server*) o en los archivos *hosts*[8] de las páginas electrónicas de bancos, cajas de ahorro, etc., a los que accede habitualmente la víctima, lo que permite conducirla a páginas electrónicas falsas, creadas expresamente por los delincuentes (*spoofing*), en las que aquélla dejara constancia de sus claves de acceso y firma electrónica[9]. Otra de las técnicas últimamente detectada es la utilización de troyanos, introducidos a través de la red en el sistema informático de la víctima mediante programas de intercambio, mensajería instantánea, correos electrónicos, que modifican la configuración del sistema informático para captar la información de las operaciones bancarias en línea (claves secretas de acceso y firma electrónica). Estos programas espía (*spyware*), que pueden permanecer ocultos durante mucho tiempo en el sistema, se activan cuando el usuario accede a las páginas de bancos u otras entidades, capturando las claves de acceso e incluso capturando las pantallas para conocer el estado de las cuentas corrientes[10]. También la obtención de claves puede realizarse a través de programas maliciosos que interceptan la información en el momento en que se introducen en la banca en línea, capturando las pulsaciones del teclado (*keyloggers*).

En la segunda fase, mediante la utilización no consentida de dichas claves se realizan traspasos patrimoniales en línea a otras cuentas bancarias situadas, generalmente, en el extranjero y previamente abiertas por otros miembros de la organización[11]. Y, finalmente, en la tercera fase, las cantidades patrimoniales transferidas de forma no consentida son retiradas rápidamente de la cuenta bancaria y enviadas por correo postal o empresas de envío de dinero a otros miembros de la organización, situados en otros estados, generalmente de la Europa del Este (Rusia, Ucrania, Estonia, Moldavia, República Checa, etc.).

Esta forma de criminalidad surge en Estados Unidos en 2003 y rápidamente se extiende por otros países. En ese país en el periodo de abril a diciembre de 2005 se detectaron 15.000 variantes de *phishing* (correos electrónicos), 8 millones de correos electrónicos enviados diariamente, alrededor 7000 páginas electrónicas falsas, en las que "picaron" el 5% de los destinatarios de los correos electrónicos masivos enviados. En 2003 el perjuicio económico causado ascendió a 2.400 millones de dólares, sólo en Estados Unidos[12]. En nuestro país, la Brigada de Investigación Tecnológica de la Comisaría General de la Policía Judicial desarticuló en 2009 una banda que defraudó alrededor de 800.000 euros mediante la técnica del *phishing*. En este año han detenido a 143 personas en nuestro país que se dedicaban a este tipo de fraudes bancarios[13].

Estas bandas constituyen verdaderas organizaciones criminales, formadas por un número considerable de personas, dotadas de una estructura organizativa, jerarquizada y de reparto bien delimitado de tareas entre sus miembros, que, generalmente, proceden de la Europa del Este y cuentan con una elevada cualificación tecnológica[14], lo que permite hablar de delincuencia

7 Otra nueva forma de criminalidad es el *smishing*, que utiliza mensajes de telefonía móvil (SMS) para la obtención del número de tarjeta y fecha de caducidad con los que posteriormente confeccionan tarjetas bancarias falsas (*skimmming*) para la compra de productos en comercios. Estas conductas quedarían recogidas actualmente en el nuevo tipo del artículo 399 bis del Código Penal, relativo a la falsificación de tarjetas bancarias, que entraría en concurso de leyes con la nueva modalidad de estafa del artículo 248.2 c) del Código Penal, que castiga como estafa cualquier operación patrimonial en perjuicio de tercero, realizada con tarjetas bancarias o con la información en ellas contenida. A estos tipos penales también responderían los supuestos de *vishing*, consistente en la copia del contenido de las bandas magnéticas (datos electrónicos) de tarjetas bancarias. Sobre las mismas v. ult. lug. cit.

8 Tanto el servidor DNS como los programas *hosts* contienen las direcciones IPs o secuencia numérica de las direcciones electrónicas (URL) de las páginas visitadas. El *pharming* cambia las direcciones IP contenidas en el servidor DNS o en el programa *host*s, conduciendo al usuario a una página electrónica diferente a la deseada.

9 V. más ampliamente, FARALDO CABANA, *Las nuevas tecnologías*, p. 91; FERNÁNDEZ TERUELO, *Cibercrimen*, p. 30. De forma similar VELASCO NÚÑEZ, *LLP* (2008), p. 21; EL MISMO, *LLP* (2007), pp. 59 y s.

10 V. más ampliamente, FERNÁNDEZ TERUELO, *Cibercrimen*, pp. 28 y s.

11 Todo ello, sin perjuicio de que con la información obtenida en la primera fase se pueda realizar otras conductas como falsificación de tarjetas bancarias (*skimming*) u operaciones de comercio electrónico no consentidas, como se ha señalado más arriba.

12 Tal y como informa en su trabajo STUCKENBERG, *ZStW* (2006), pp. 878 y ss.

13 Tal y como informa el Ministerio del Interior en una nota de prensa de 16 de mayo de 2010. V. http://www.mir.es/DGRIS/Notas_Prensa/Policia/2010/np051601.html VELASCO NÚÑEZ, *LLP* (2007), p. 58 señala que el 75% de las claves obtenidas por alguna de estas técnicas son utilizadas por los *phishers* o *scammers* para la realización de transferencias bancarias no consentidas, mientras que el 25% restante se emplea en otro tipo de fraudes como subastas por Internet o compras electrónicas.

14 En este sentido v. VELASCO NÚÑEZ, *LLP* (2007), p. 62; EL MISMO, *LLP* (2008), p. 21. También resulta muy ilustrativo el Auto AP Barcelona de 23 de octubre de 2009.

organizada, altamente cualificada e internacional[15]. Siendo Internet el medio a través del cual se realiza esta nueva forma de criminalidad, el perjuicio patrimonial presenta un alcance global e internacional por el hecho de que los ataques son masivos y las víctimas, numerosas, se encuentran repartidas por todo el mundo. El carácter transnacional de estas conductas también responde a su propia ejecución, ya que las diferentes fases se realizan en estados diferentes para dificultar su descubrimiento y persecución[16]. Por otro lado, el hecho de que se lleven a cabo no de forma aislada, sino a través de ataques masivos con un elevado perjuicio económico permite configurarlos a efectos penológicos como delitos masa.

La mera participación en estas organizaciones criminales supondría de entrada la comisión de los nuevos tipos de los artículos 570 bis del Código Penal, introducidos por la LO 5/2010, de 22 de junio, por la que se modifica el Código Penal[17]. Conforme al artículo 570 bis 1, la organización criminal es toda "agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos, así como llevar a cabo la perpetración reiterada de faltas", lo que dificulta su delimitación con la asociación ilícita recogida en el artículo 515.1º del Código Penal, con el que entraría en concurso de leyes[18/19]. El Código Penal resuelve este concurso a favor de la organización criminal con base en el principio de alternatividad (art. 570 quater 2). El delito del artículo 570 bis será de aplicación, con independencia de que la organización se haya constituido, esté asentada o desarrolle su actividad en el extranjero, siempre que lleve a cabo cualquier acto penalmente relevante en España (art. 570 quater 3 CP).

A este delito habría que añadir la responsabilidad penal por los atentados contra el patrimonio, la intimidad, y, en su caso, la fe pública. Si bien las dos primeras fases son llevadas a cabo por diferentes miembros de la organización, la tercera la realizan los denominados "muleros", que no siempre cuentan con un conocimiento global de la operación[20]. De ser realizadas las dos primeras fases por los mismos sujetos, cabría establecer una responsabilidad penal por un concurso de delitos, excepcionalmente de leyes, dado que tales conductas no sólo lesionan el patrimonio, sino también la intimidad o la fe pública. En efecto, en la primera fase, las modalidades del *spyware* y *pharming* podrían suponer un delito contra la intimidad del artículo 197 del Código Penal, mientras que las de *pharming* y *phishing* un atentado contra la fe pública por falsificación documental, siempre que éstos respondan al concepto de documento del artículo 26 del Código Penal[21].

Se ha planteado la posibilidad de reconducir los supuestos de *phishing* por una estafa común del artículo 248.1, dado que el envío del mensaje electrónico fraudulento podría constituir el engaño psicológico del que parte esta modalidad de estafa. Sin embargo, esta solución no resulta adecuada, puesto que, por un lado,

15 También así la califican las sentencias del Tribunal Supremo de de 12 de junio de 2007 y de 16 de marzo de 2009.

16 Sobre los posibles conflictos de jurisdicción penal que ello puede implicar v. mi trabajo, «Delitos transfronterizos en Internet: aspectos problemáticos» en *La adaptación del Derecho Penal al desarrollo social y tecnológico*: C. M. Romeo Casabona y F. G. Sánchez Lázaro, Comares, Granada (en prensa).

17 Resultado de la transposición de la Decisión Marco 2008/841/JAI, de 24 de octubre, del Consejo de Europa sobre la Lucha contra la Delincuencia Organizada.

18 La organización criminal parece más adecuada en estos casos que la de asociación ilícita del art. 515 del Código Penal, definida por la doctrina y jurisprudencia como la unión de un mínimo dos o tres personas para la realización de alguno de los fines del art. 515, entre los que se encuentra la comisión de delitos (número 1), dotada de una estructura organizativa y de cierta permanencia en el tiempo. Con anterioridad a la reforma mencionada, VELASCO NÚÑEZ, *LLP* (2007), p. 62 defiende la concurrencia de este tipo en los supuestos analizados. I. SÁNCHEZ GARCÍA DE PAZ, *Comentarios al Código Penal*: M. Gómez Tomillo (Dir.), Lex Nova, Valladolid, 20010, pp. 1795 y 1922, delimita una y otra en atención a si la unión o agrupación de personas concertadas para la comisión de delitos constituye una asociación ilícita o no, pues entiende que las conductas del art. 515 constituyen una manifestación del abuso del derecho de asociación. Planteando diversos criterios y la dificultades de delimitación v. C. MARTELL PÉREZ-ALCALDE y DÉBORA QUINTERO GARCÍA, «*De las organizaciones y grupos criminales*» en *La Reforma Penal de 2010: Análisis y Comentarios*: G. Quintero Olivares (Dir.), Aranzadi/Thomson Reuters, 2010, pp. 360 y s.

19 En cambio, no sería de aplicación el tipo del art. 570 ter c), referido al grupo criminal definido como la unión de más de dos personas que tenga por finalidad o por objeto la perpetración concertada de delitos o la comisión concertada y reiterada de faltas, pero no reúna alguna o algunas de las características de la organización criminal. Tales características no pueden ser otras que la estabilidad y la estructura organizada.

20 Sobre esta cuestión v. VELASCO NÚÑEZ, *LLP* (2007), p. 62 y la STS de 12 de junio de 2007 (FJ segundo).

21 En este sentido v. VELASCO NÚÑEZ, *LLP* (2007), p. 61.

la posible víctima tan sólo entrega sus claves bancarias, pero no realiza por si misma el acto de disposición patrimonial exigido en el tipo de lo injusto. Y, por otro lado, resulta discutible que el correo electrónico fraudulento constituya un engaño idóneo que permitiese castigar tales comportamientos, al menos, en grado de tentativa[22]. Téngase en cuenta que muchos de estos correos electrónicos son enviados desde el extranjero con una incorrecta redacción y traducción, y de forma masiva a usuarios de la red, que en la mayoría de las ocasiones no disponen de cuentas bancarias en la entidad que supuestamente ha remitido el mensaje. Por otro lado, resulta cuestionable que esta conducta, aun cuando permita acceder a las claves de acceso de la cuenta bancaria en línea de un tercero, pueda presentarse como un engaño bastante para configurar una estafa común, dado que por si misma no dará lugar en ningún caso al acto de disposición patrimonial exigido en el tipo.

Más difícil sería, en mi opinión, la aplicación del tipo de lo injusto del 248.2 b), que castiga, entre otras conductas, la posesión de programas informáticos destinados a la comisión de estafas, puesto que las aplicaciones o programas informáticos utilizados en el *spyware* (programa espía) o *pharming*, a pesar de que pueden ponerse al servicio de la ejecución de estafas, no pueden ser considerados como "programas específicamente destinados a la comisión de estafas", tal y como exige el precepto[23]. No obstante, de concurrir entraría en concurso de leyes con la estafa recogida en el 248.2 a) del Código Penal, resolviéndose a favor de éste último.

En este trabajo me ocuparé de la respuesta que ofrece nuestro Código Penal a la conducta llevada a cabo en la segunda fase; esto es, la utilización no consentida de claves de acceso a cuentas bancarias y firma electrónica para realizar con ánimo de lucro transferencias bancarias en línea con el consiguiente perjuicio patrimonial de terceros.

En atención al bien jurídico lesionado estas conductas constituyen básicamente un atentado contra el patrimonio, pero cabe plantearse si esta fase supone asimismo un atentado contra la intimidad previsto en el tipo del artículo 197.2 del Código Penal. Este precepto castiga, entre otras conductas la utilización, en perjuicio de tercero, de datos reservados de carácter personal de otro que se hallen registrados en ficheros o soportes informáticos o electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. La punición de los comportamientos objeto de este trabajo —la realización de transferencias bancarias en línea no autorizadas, mediante la utilización no consentida de datos personales de terceros— a través de este precepto dependería de que las claves bancarias y firma electrónica pudieran ser considerados datos reservados de carácter personal[24], y de que el tipo admitiese la mera utilización de datos personales de carácter electrónico, sin necesidad de que éstos formasen parte de un fichero, archivo o registro (electrónico, informático o telemático)[25]. No obstante, de concurrir este tipo cabe plantearse si entraría en concurso de delitos o de leyes con el posible atentado contra el patrimonio de carácter defraudatorio, como veremos en el siguiente apartado. La solución por una u otra opción dependerá del alcance del elemento subjetivo de lo injusto "en perjuicio de tercero", que para unos se reduce al ánimo de atentar contra la intimidad[26], mientras que para otros puede ir dirigido tanto a aspectos relacionados con la intimidad como a otros intereses de naturaleza económica[27].

22 En el mismo sentido FARALDO CABANA, *Las nuevas tecnologías*, pp. 91 y s.; J. P. GRAF, «Phishing derzeit nicht generell strafbar» en *NStZ* (3) 2007, pp. 130 y s.; M. GERCKE, «Die Strafbarkeit von "Phishing" und Identitätsdiebstahl» en *Computer und Recht* (8), 2005, p. 608. Plantean la posibilidad de la tentativa FERNÁNDEZ TERUELO, *Cibercrimen*, p. 43 y VELASCO NÚÑEZ, *LLP* (2008), p. 22; STUCKENBERG, *ZStW* (118), 2006, pp. 898 y s. La respuesta sería la misma en los supuestos de *smishing* en los que el engaño se realiza a través de SMS.

23 En el mismo sentido críticamente v. J. G. FERNÁNDEZ TERUELO, *Comentarios a la Reforma Penal de 2010*: F. J. Álvarez García y J. L. González Cussac (Dirs.), Tirant lo Blanch, Valencia, 2010, p. 279; R. M. MATA Y MARTÍN, *Comentarios al Código Penal*: M. Gómez Tomillo (Dir.), Lex Nova, Valladolid, 2010, p. 970.

24 A favor VELASCO NÚÑEZ, *LLP* (2008), p. 23; FERNÁNDEZ TERUELO, *Cibercrimen*, pp. 126 y s.

25 En contra F. MORALES PRATS, *Comentarios a la Parte Especial del Código Penal*: G. Quintero Olivares (Dir.) (8ª ed.), Aranzadi y Thomson Reuters, 2009, p. 422; M. A. RUEDA MARTÍN, *Protección penal de la intimidad personal e informática:(los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, Atelier, Barcelona, 2004, p. 71; C. M. ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia, 2004, Tirant lo Blanch, Valencia, 2004, p. 114. A favor VELASCO NÚÑEZ, LLP (2007), p. 61.

26 De esta opinión MORALES PRATS, *Comentarios a la Parte Especial*, pp. 424 y s.

27 Así ROMEO CASABONA, *Los delitos de descubrimiento*, p. 114.

II

La utilización no consentida de claves de acceso a cuentas bancarias y firma electrónica para realizar con ánimo de lucro transferencias bancarias en línea con el consiguiente perjuicio patrimonial de terceros constituye en esencia un ataque contra el patrimonio, como ya se ha señalado. En este apartado trataré de determinar si alguno los actuales tipos penales pueden cubrir satisfactoriamente estas conductas o, si por el contrario, es necesaria su reforma o incluso la incorporación de nuevos delitos que cubran las actuales insuficiencias.

Teniendo en cuenta que esta nueva forma de criminalidad contra el patrimonio se caracteriza por la concurrencia de ánimo de lucro por parte de sus autores, debemos comenzar por el grupo de los delitos de enriquecimiento. Dado que estas conductas consisten en transferencias patrimoniales, quedan descartados los delitos de apoderamiento, que parten de la sustracción de una cosa mueble ajena sin la voluntad de su titular. Ello nos llevaría a los delitos de defraudación y, más concretamente, a las estafas.

Mayoritariamente se defiende que estos supuestos no responden a una estafa común del artículo 248.1 del Código Penal, puesto que la conducta del sujeto activo no se inicia con un engaño a otra persona, sino, en todo caso, con un "engaño" a una máquina: el sistema informático de la banca en línea[28]. Y, por otro lado, tampoco contamos con un acto de disposición patrimonial por parte de un tercero que ha caído en un error a consecuencia del engaño. La nueva modalidad de estafa del artículo 248.2 c) del Código Penal, introducida por la LO 5/2010, de 22 de junio, tampoco puede ser aplicada a estos casos, dado que las operaciones patrimoniales en perjuicio de tercero llevadas a cabo a través de Internet ni son realizadas con tarjetas bancarias o cheques de viajes, ni con la información en ellos contenida[29]. En nuestro supuesto de hecho el sujeto activo si bien utiliza ilícitamente las claves de acceso a una cuenta bancaria y firma electrónica, dicha información no se corresponde con la contenida en la tarjeta bancaria, aun cuando el titular y la cuenta bancaria a la que está sujeta la tarjeta sean los mismos.

En cambio, esta nueva forma de criminalidad podría responder al fraude informático recogido en el artículo 248.2 a) del Código Penal[30], que establece: "*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 otro*". El supuesto de hecho objeto de análisis se asemeja bastante a este tipo delictivo. Además de concurrir el tipo subjetivo exigido por este tipo de lo injusto, ánimo de lucro y el dolo correspondiente, contamos en el tipo objetivo con una transferencia no consentida de un activo patrimonial y el consiguiente perjuicio (patrimonial) de un tercero (de otro). La completa subsunción de la conducta en esta figura delictiva dependerá de si concurre el medio comisivo: la manipulación informática o el artificio semejante, mediante los cuales se consigue la transferencia patrimonial no consentida, en perjuicio de otro.

El Código Penal no define ni la manipulación informática ni el artificio semejante a aquélla. Para la doctrina mayoritaria la manipulación informática consiste en la manipulación de datos automatizados a través de la introducción, supresión o alteración de datos falsos, o la manipulación de las instrucciones del programa informático para alterar el resultado del tratamiento automatizado de los mismos, que en el fraude informático, debe ocasionar el traspaso patrimonial ilícito[31]. Esta definición es seguida asimismo por la jurisprudencia[32].

28 Así, entre otros, FERNÁNDEZ TERUELO, *Cibercrimen*, p. 43. En cambio, el engaño a una persona si concurriría en el *phishing*, tal y como hemos mencionado más arriba, aunque en tales casos a lo sumo cabría establecer una responsabilidad penal en grado de tentativa.

29 Este nuevo tipo penal ya formaba parte del Proyecto de Ley Orgánica por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, de 15 de enero de 2007, pero no así del Anteproyecto de Ley Orgánica por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, de 27 de octubre de 2008.

30 Este precepto también ha sido modificado por la LO 5/2010, de 22 de junio. Se sustituye "en perjuicio de tercero" por "en perjuicio de otro" y se mejora la ortografía del texto, además de cambiar su numeración. Cambios que, en mi opinión, son irrelevantes para su interpretación.

31 Así, C. M. ROMEO CASABONA, *Poder informático y seguridad jurídica: la función tutelar del Derecho Penal ante las nuevas tecnologías de la información*, Fundesco, Madrid, 1988, p. 47; J. A. CHOCLÁN MONTALVO, «Infracciones patrimoniales en los procesos de transferencia de datos» en *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*: C. M. Romeo Casabona (Coord.), Comares, Granada, 2006*El Cibercrimen*, pp. 72 y s.; EL MISMO, *El delito de estafa*, Bosch, Madrid, 2000, pp. 302 y ss.; FERNÁNDEZ TERUELO, *Cibercrimen*, p. 45; A. ARROYO DE LAS HERAS, *Los delitos de estafa y falsedad documental*, Bosch, Barcelona, 2005, pp. 65 y ss.; R. MATA Y MARTÍN, *Delincuencia informática y Derecho Penal*, Edisofer, Madrid, 2001, p. 48; E. ORTS BERENGUER y M.

La manipulación en la entrada de datos consistiría en suministrar datos falsos al ordenador, bien mediante modificación de los reales ya contenidos en el sistema, bien introduciendo datos completamente ficticios, bien omitiendo el registro de datos reales (deudas, cargos, etc.). En tales casos el tratamiento informatizado de datos y el resultado es correcto, pero ficticio dado que los datos de partida (introducidos, suprimidos o alterados) no se corresponden con los reales[33]. Otra de las modalidades de manipulación informática consistiría en la alteración o manipulación de los elementos físicos del sistema informático[34]. En cambio, son rechazadas las manipulaciones anteriores a la introducción de los datos (*input*) como las posteriores a la salida de los mismos (*output*)[35].

Por artificio semejante se ha entendido todo truco, enredo, artimaña o técnica defraudatoria sobre sistemas informáticos o mecánicos, causal e idónea para producir directamente el traspaso no consentido de activos patrimoniales[36].

Cabe plantearse en qué momento se produciría la manipulación informática o el artificio semejante del que deriva el traspaso patrimonial no consentido con el consiguiente perjuicio económico en el modelo de criminalidad que estamos analizando. ¿En la primera fase, con la obtención ilícita de las claves a través de una aplicación informática espía, propia del *spyware*, o con la modificación de direcciones DNS o los archivos *hosts* que contienen las direcciones IPs, propia del *pharming*, o con la falsificación de páginas electrónicas del *phishing* y *pharming*; o en la segunda fase, con la utilización no consentida de las claves de acceso a la cuenta bancaria y firma electrónica para la realización de la transferencia no autorizada, o con la propia transferencia bancaria no autorizada?

Aunque en este trabajo mi objetivo es el análisis jurídico-penal de la segunda fase de estas conductas, resulta adecuado establecer si el acceso no consentido a estas claves en la modalidad de *spyware* o *pharming* de la primera fase se lleva a cabo mediante una manipulación informática o artificio semejante idóneos para lograr el traspaso patrimonial de la segunda fase, pues en ese caso ambas fases darían lugar a responsabilidad penal por un delito de fraude informático del artículo 248.2 a) del Código Penal.

Entiendo que tanto en la modalidad de *pharming* como en la de *spyware* podría darse una manipulación informática o, al menos, un artificio semejante a aquélla en el acceso ilícito a las claves bancarias y firma electrónicas de un tercero. En el primer caso la manipulación informática consistiría en la modificación de las direcciones DNS o de los archivos en el que se encuentran localizadas las direcciones IPs de páginas que habitualmente utiliza la víctima (bancos, compañías de transporte, comercios, etc.), que supondría la introducción de datos falsos (nuevas direcciones DNS o IPs). En el *spyware*, si bien la utilización de la aplicación informática espía no responde al concepto de manipulación informática apuntado, dado que no constituye ni alteración de datos automatizados, ni modificación de las instrucciones del programa informático para alterar el resultado del tratamiento automatizado de los datos, pero sí podría responder al de artificio semejante a la manipulación informática. La introducción a través de la red de una aplicación espía en el sistema informático de un tercero con la finalidad de localizar las claves de acceso a la banca electrónica se presenta como la maquinación, truco o enredo defraudatorio sobre un sistema informático propio del concepto de artificio se-

ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001, p. 64. Sobre los diferentes conceptos propuestos, v. MATA Y MARTÍN, «Medios electrónicos de pago y delitos de estafa» en *Los medios electrónicos de pago. Problemas Jurídicos*: R. Mata y Martín (Dir.), Comares, Granada, 2007, pp. 343 y ss. (345).

32 V. por todas la STS de 20 de noviembre de 2001 (f. j. único, apartado 3) "La actual redacción del artículo 248.2 del Código Penal permite incluir en la tipicidad de la estafa aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de órdenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia". (...) "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". Más ampliamente sobre la posición jurisprudencial FERNÁNDEZ TERUELO, *Cibercrimen*, p. 48.

33 Al respecto v. por todos CHOCLÁN MONTALVO, *El Cibercrimen*, pp. 77 y s.

34 V. STS de 20 de noviembre de 2001, ya citada.

35 Así, MATA Y MARTÍN, *Delincuencia informática*, p. 51; ARROYO DE LAS HERAS, *Los delitos de estafa*, p. 72.

36 Así, A. GALÁN MUÑOZ, *El fraude y la estafa mediante sistemas informáticos*, Tirant lo Blanch, Valencia, 2005, p. 566; CHOCLÁN MONTALVO, *El delito de estafa*, Bosch, Madrid, 2000, pp. 302 y s. Reduciéndolo a sistemas informáticos, v. FARALDO CABANA, *Las nuevas tecnologías*, pp. 88 y 97; MATA Y MARTÍN, *Los medios electrónicos de pago*, p. 348.

mejante. No obstante, en tales supuestos, y a diferencia de los tradicionales, la manipulación informática o, en su caso, el artificio semejante utilizado por el sujeto activo no da lugar directamente al traspaso patrimonial en perjuicio de tercero, sino tan sólo permite acceder a las claves de acceso y firma electrónica, que posibilitarán posteriormente al sujeto activo llevar a cabo la transferencia patrimonial no consentida en una segunda acción.

¿Pero responden estos supuestos al medio comisivo del artículo 248.2 a)? En principio, la fórmula genérica del tenor literal no parece impedirlo, pues el tipo no exige que la manipulación informática directamente provoque la transferencia patrimonial no consentida, sino tan sólo que valiéndose de una manipulación informática o artificio semejante se consiga una transferencia patrimonial no consentida; esto es, que entre la manipulación informática (o el artificio semejante) y la transferencia ilícita exista una relación de causalidad y que aquélla sea idónea para lograrlo[37]. Así también ha sido entendido por los tribunales que califican tales supuestos de fraude informático, aunque sin entrar en el fondo de la cuestión[38]. No obstante, de acuerdo con el concepto restringido de manipulación informática, que mantiene la doctrina mayoritaria, tan sólo aquélla que directamente ocasiona el traspaso patrimonial ilícito y el consiguiente perjuicio de tercero constituye el medio comisivo del fraude del artículo 248.2 a). De esta forma las manipulaciones en el sistema informático propias del *spyware* y del *pharming* tendentes a la obtención subrepticia de las claves de acceso a las cuentas bancarias, y no directamente al traspaso patrimonial no consentido, no constituirían la manipulación propia del fraude informático de este precepto. Se trataría de supuestos de manipulación informática previos a la introducción de datos que, junto a las realizadas con posterioridad a la salida de datos automatizados, quedarían fuera del concepto mantenido[39]. Y entiendo que a la misma respuesta nos conduciría el concepto de artificio semejante defendido por la doctrina mayoritaria, aunque sobre este punto nada se ha dicho al respecto. Consecuentemente, de la definición mayoritariamente defendida se desprendería que conforme al artículo 248.2 a) tan sólo se admitiría la manipulación informática que directamente diera lugar al traspaso patrimonial no consentido en perjuicio de un tercero. No respondiendo estas modalidades a los conceptos restringidos de manipulación informática y artificio semejante, el fraude informático quedaría excluido de la primera fase de esta nueva forma de criminalidad. Todo ello sin perjuicio, claro está, de que tales comportamientos pudieran dar lugar a responsabilidad penal por atentado a la intimidad o la fe pública, como ya se ha apuntado[40].

III

Planteada la dificultad de que la manipulación informática de la primera fase de las defraudaciones patrimoniales en la red se adecue a la exigida en el tipo del fraude informático, analizaremos la posibilidad de si este elemento del tipo de lo injusto está presente en la segunda fase, a través del propio traspaso patrimonial no consentido o, en su caso, mediante la utilización no autorizada de las claves bancarias y firma electrónica, aspectos que son comunes a todas las modalidades de la primera fase (*phishing, pharming y spyware*).

De acuerdo con el concepto de manipulación informática que mayoritariamente se mantiene no parece que la simple introducción del número de la cuenta corriente destinataria y de los datos correspondientes a la operación (cantidades, etc.) del traspaso patrimonial responda a ese concepto, dado que los datos introducidos en el sistema informático no son datos falsos, sino simplemente representan una operación patrimonial no autorizada[41]. En cambio, si la transferencia patrimonial se justificase en la prestación de un servicio, compra o crédito ficticio, no se podría negar la concurrencia de la manipulación informática por introducción de datos

37 También defendiendo un concepto amplio de manipulación informática y artificio semejante en el tipo del artículo 248.2 a) v. FARALDO CABANA, *Las nuevas tecnologías*, pp. 90, 100, 102 y 104; J. M. VALLE MUÑIZ y G. QUINTERO OLIVARES, *Comentarios a la Parte Especial del Derecho Penal*: G. Quintero Olivares (Dir.) (8ª ed.), Aranzadi y Thomson Reuters, 2009, pp. 649 y s. En el mismo sentido v. la STS de 30 de mayo de 2009 (FJ tercero). Críticamente CHOCLÁN MONTALVO, *El Cibercrimen*, p. 70.

38 V. STS de 12 de junio de 2007 (FJ segundo). En cambio, la STS de 16 de marzo de 2009 (FJ 6) mantiene la condena de la instancia inferior por estafa común del artículo 248.1 en un supuesto de *phishing*. V. también la SAP de Madrid de 22 de enero de 2009, que castiga por el 248.2. a) un supuesto de *pharming* y la SAP de Vizcaya de 9 de mayo de 2006, que recoge un supuesto de *spyware*.

39 Así, MATA Y MARTÍN, *Delincuencia informática*, p. 51; ARROYO DE LAS HERAS, *Los delitos de estafa*, p. 72.

40 Al respecto v. FERNÁNDEZ TERUELO, *Cibercrimen*, p. 51 y VELASCO NÚÑEZ, *LLP* (2008), p. 23; EL MISMO, *LLP* (2007), p. 61.

41 Así lo entienden, entre otros, FERNÁNDEZ TERUELO, *Cibercrimen*, pp. 47 y 52.

falsos. Entonces cabe plantearse por qué no se admite si dicho traspaso patrimonial ilícito se deja sin justificar en un concepto determinado (prestación de servicios, compras, etc.), dado que las conductas serían en esencia las mismas. No me parece adecuada la posición de la doctrina al respecto. En mi opinión, en tales supuestos debería admitirse la presencia de una manipulación informática, teniendo en cuenta que los datos que se introducen en el sistema no han sido autorizados por el titular de la cuenta, debiendo considerarse a estos efectos como introducción de datos falsos[42].

Conforme a este concepto restringido de manipulación informática, un sector de la doctrina rechaza igualmente que la introducción no autorizada de las claves de acceso a la cuenta bancaria en línea y de la firma electrónica constituya una manipulación propia del artículo 248.2 a), puesto que tales datos ni son falsos, ni son alterados, sino tan sólo utilizados sin consentimiento de su titular[43]. Y se propone por ello la modificación del precepto para incorporar estos nuevos supuestos[44].

De acuerdo con lo ya expuesto, entiendo que la utilización ilícita de dicha información podría constituir una manipulación informática o, al menos, un artificio semejante a aquélla[45]. Esta interpretación, si se quiere extensiva, del medio comisivo del artículo 248.2 a) está justificada tanto en la interpretación objetiva como teleológica del precepto[46]. De su tenor literal no cabe deducir que la manipulación informática se reduzca a una alteración del proceso de datos automatizados[47], como tradicionalmente se ha defendido, sino que es mucho más amplia, debiendo entenderse como toda maquinación o maniobra sobre un sistema informático[48]. El hecho de que el supuesto que diese origen al tipo del artículo 248.2 fuese el de introducción de datos falsos y alteración del programa informático y de que el concepto de manipulación informática del precepto defendido por doctrina y jurisprudencia se identificase con estos supuestos no constituyen razones suficientes para seguir manteniendo tal interpretación restrictiva, sobre todo si tenemos en cuenta el concepto de manipulación informática acogido en tratados internacionales y en otros ordenamientos jurídicos y las nuevas formas de criminalidad contra las que nos enfrentamos[49]. Por otro lado, la voluntad de la ley ha sido la de dar cobertura a todo tipo de fraude patrimonial similar a los que en su momento sirvieron de base al precepto, de ahí que el legislador haya optado por una fórmula genérica

42 En este sentido se ha pronunciado el Tribunal Supremo en la sentencia de 20 de noviembre de 2001 (FJ único. 3) que sitúa entre las modalidades de manipulación informática del actualmente artículo 248.2 a) la creación de órdenes de pago o de transferencias.

43 De esta opinión O. MORALES GARCÍA, «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248)» en *La Reforma Penal de 2010: Análisis y Comentarios*: G. Quintero Olivares (Dir.), Aranzadi/Thomson Reuters, 2010, p. 192; ARROYO DE LAS HERAS, *Los delitos de estafa*, p. 72; FERNÁNDEZ TERUELO, *Cibercrimen*, pp. 47, 49 y s., 52; CHOCLÁN MONTALVO, *El Cibercrimen*, p. 75; MATA Y MARTÍN, *Los medios electrónicos de pago*, p. 346. Cft. STS de 30 de mayo de 2009 (FJ tercero). Sin embargo, la sentencias de la AP de León de 3 de noviembre de 2008 (FJ tercero), de la AP de Madrid de 21 de diciembre de 2004 (FJ segundo) y de la AP de Navarra de 10 de mayo de 2006 (FJ segundo) condenan tales supuestos de transferencia bancaria no consentida en línea como fraude informático.

44 Así, FERNÁNDEZ TERUELO, *Cibercrimen*, p. 52, para el que el art. 248.2 a) del Código Penal debería castigar la "ejecución, con ánimo de lucro, de operaciones informáticas no autorizadas perjudiciales para el patrimonio de otro". No obstante, en un trabajo posterior cambia de posición y admite que estos comportamientos deben responder por el tipo de estafa informática del art. 248.2 a) del Código Penal. V. FERNÁNDEZ TERUELO, *Comentarios a la Reforma Penal de 2010*, pp. 280 y s.

45 También así, T. S. VIVES ANTÓN, E. ORTS BERENGUER, J. C. CARBONELL MATEU, J. L. GONZÁLEZ CUSSAC y C. MARTÍNEZ-BUJÁN PÉREZ, *Derecho Penal. Parte Especial* (3ª ed. Revisada) Tirant lo Blanch, Valencia, 2010, Lección XXIV.

46 También a favor de una interpretación extensiva del precepto v. FARALDO CABANA, *Las nuevas tecnologías*, pp. 88 y ss. y FERNÁNDEZ TERUELO, *Comentarios a la Reforma Penal de 2010*, pp. 280 y s., modificando su posición anterior.

47 En el Diccionario de la lengua española de la Real Academia Española se define manipulación como acción y efecto de manipular, que puede entenderse en este contexto como intervenir con medios hábiles e incluso arteros en la política, información, mercado, etc., con distorsión de la verdad y la justicia, y al servicio de intereses particulares. Asimismo, se utiliza este verbo de forma coloquial para significar que alguien se mezcla en los negocios ajenos.

48 Como también ha puesto de manifiesto el Tribunal Supremo, entre otras, en la sentencia de 21 de noviembre de 2001, ya comentada.

49 También el Convenio Europeo sobre Criminalidad del Consejo de Europa, de 23 de noviembre de 2001, establece en su artículo 8 una propuesta de regulación de la estafa informática de carácter amplio. "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: a. la introducción, alteración, borrado o supresión de datos informáticos. b. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero".

tan amplia para castigar la estafa informática; esto es, la utilización de conceptos normativos no definidos en la ley, previendo con ello el castigo de nuevas formas de defraudación patrimonial como las actuales[50]. En mi opinión bajo el tipo del artículo 248.2 a) cabría castigar cualquier maniobra, truco o ardid sobre un sistema informático o mecánico que permitiese un traspaso patrimonial no consentido, dado que no define la manipulación informática, como así se ha hecho en otros ordenamientos como el alemán, y porque además la acompaña de otro medio comisivo como es el artificio semejante a aquélla, que tampoco define. Una fórmula tan amplia como ésta admitiría los supuestos de autentificación falsa ante un sistema informático de nuestro objeto de estudio, pero también otros, como la propia conducta de creación de órdenes de pago o traspaso no autorizadas, o incluso, aunque con las reservas más arriba apuntadas, el acceso ilícito a las claves bancarias o números secretos de cuentas. Asimismo, el artificio semejante a la manipulación informática del precepto también admitiría tales conductas[51]. Por ello, se podría considerar que si la maquinación, truco o ardid, etc. se realiza sobre un sistema informático o mecánico, a través de alteración de datos en el sistema a la entrada o salida, con alteración del programa informático o del sistema informático o mecánico, como de cualquier otra forma no originariamente pensada, concurriría, al menos, el artificio semejante a la manipulación del tipo de lo injusto. No obstante, por razones de seguridad jurídica y con base en las exigencias de certeza y taxatividad propias del principio de legalidad sería conveniente que el medio comisivo del precepto se definiese o, al menos, se concretase[52].

Contribuye también a la posición aquí defendida, la regulación de la estafa informática de otros ordenamientos jurídicos, como por ejemplo el alemán, cuyo § 263 a del StGB[53], si bien tiene una formulación más concreta y delimitada que nuestro 248.2 a), entre ellas incluye expresamente tanto la utilización ilícita de datos como cualquier tipo intervención no autorizada, que interfiera en el resultado de un tratamiento de datos con la intención de obtener un beneficio patrimonial ilícito para si o para un tercero y en perjuicio del patrimonio de otro. Con tal formulación el castigo de esta nueva forma de criminalidad de atentados al patrimonio en la banca en línea que estamos analizando no ofrece problemas[54].

En nuestro país también se ha incorporado esta fórmula de utilización ilícita de determinada información para realizar operaciones patrimoniales en perjuicio de tercero en el artículo 248.2 c), introducido por la LO 5/2010, de 22 de junio, de reforma del Código Penal. Como ya he adelantado, este apartado castiga expresamente como estafa las operaciones patrimoniales en perjuicio de tercero mediante la utilización de tarjetas bancarias o cheques de viaje o de los datos en ellos contenidos[55]. Pero, por otro lado, lo regula de forma independiente al tradicional fraude informático (apartados a y c del artículo 248.2, respectivamente), lo que podría indicar que para el legislador la utilización ilícita de información contenida, por ejemplo, en las tarjetas de crédito en perjuicio de tercero no constituye un fraude informático, dado que a diferencia del precepto alemán, nuestro nuevo artículo 248.2 introduce esta nueva modalidad en un apartado independiente (apartado c) a aquél que recoge el supuesto tradicional de

50 En el mismo sentido FARALDO CABANA, *Las nuevas tecnologías*, p. 88.

51 Si artificio semejante debiese contener el sentido de ardid o engaño equivalente a la manipulación quedaría vacío de contenido y sería superfluo, salvo que lo identificásemos con manipulación mecánica (máquinas de bebida, de acceso al metro, cabinas de teléfono, etc.).

52 También críticamente, entre otros, FARALDO CABANA, *Las nuevas tecnologías*, p. 88; VELASCO NÚÑEZ, *LLP* (2008), p. 24.

53 El que con la intención de obtener un beneficio patrimonial ilícito para sí o para un tercero, lesiona el patrimonio de otro interfiriendo en el resultado de un tratamiento de datos, mediante una estructuración incorrecta del programa, la utilización incorrecta o incompleta de datos, la utilización de datos sin autorización, o la intervención de cualquier otro modo no autorizado en el proceso, será castigado con la pena de privación de libertad de hasta cinco años o con multa.

54 V. T. FISCHER, *StGB und Nebengesetze* (56 Aufl.), C. H. Beck, München, 2009, § 263 a Rn 11a; G. DUTTGE, *Nomos Kommentar*, Nomos, Baden-Baden, 2008, § 263 a Rn 20; P. CRAMER y W. PERRON, *Schönke/Schröder Strafgesetzbuch Kommentar* (27 Aufl.), C. H. Beck, München, 2006, § 263 a Rn 14.

55 Con este nuevo apartado el legislador se decanta por la posición mantenida por la jurisprudencia y un sector de la doctrina al considerar como fraudes y no robo con fuerza en las cosas los atentados al patrimonio mediante la utilización abusiva de tarjetas bancarias o los datos contenidos en ellas. Al respecto v., entre otras, las sentencias del Tribunal Supremo de 20 de noviembre de 2001 y de 21 de diciembre de 2004. Asimismo, v. CHOCLÁN MONTALVO, *El Cibercrimen*, pp. 76 y s. en relación con el supuesto de hecho de la STS de 20 de noviembre de 2001, cambiando de opinión respecto a otros trabajos. V. «Fraude informático y estafa por computación» en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial X (2001), p. 345; EL MISMO, *El delito de estafa*, pp. 309 y ss. También a favor de considerar estos casos como manipulación informática ORTS BERENGUER y ROIG TORRES, *Delitos informáticos*, p. 67.

fraude informático (apartado a)[56]. Por otro lado, resulta lamentable e incomprensible que esta nueva modalidad de estafa se haya reducido a la utilización de tarjetas bancarias y cheques de viaje, dejando fuera las nuevas formas de fraude cometidas a través la red, dado que tales operaciones patrimoniales en perjuicio de tercero ni son realizadas con tarjetas bancarias o cheques de viajes, ni con la información en ellos contenida[57]. Como ya adelanté, la información utilizada ilícitamente en estos supuestos (claves de acceso a una cuenta bancaria y firma electrónica) no se corresponde con la contenida en la tarjeta bancaria, aun cuando el titular y la cuenta bancaria a la que está sujeta la tarjeta sean los mismos.

Asimismo, la postura mantenida en este trabajo es la que vienen manteniendo los tribunales españoles en relación con esta nueva forma de criminalidad, al castigarla mayoritariamente por fraude informático, aunque si bien es cierto, sin entrar en el fondo de la cuestión[58].

Por otro lado, ésta es la posición que defiende actualmente el Tribunal Supremo y un sector de la doctrina en un caso similar de utilización ilícita de tarjetas bancarias en cajeros automáticos o comercios[59]. En relación con estos supuestos defiende actualmente el Tribunal Supremo que la introducción del número de identificación personal (PIN) de la tarjeta bancaria en el sistema informático del cajero o en el terminal de un punto de venta (TPV) por persona no autorizada constituye una manipulación informática, cuando no un artificio semejante a aquélla, propios del fraude informático recogido en el artículo 248.2 a) del Código Penal[60]. Señala así que tales conductas de uso abusivo, no autorizado, del PIN de las tarjetas bancarias constituyen un artificio semejante a la manipulación informática, desde el momento en que el sujeto activo aparenta ante el sistema ser el titular de la tarjeta o, en su caso, cuenta bancaria, logrando el funcionamiento del sistema informático o mecánico (cajero o terminal de punto de venta) sin la debida autorización o en forma contraria a deber[61]. Incluso en alguna sentencia, mantiene que la identificación ante el sistema como titular de la tarjeta o cuenta mediante la utilización del número secreto u otras claves daría lugar a una manipulación informática propia del artículo 248.2 a), dado que se introducen datos falsos en el sistema: "se oculta la identidad real del operador y se suplanta al verdadero titular"[62].

56 Con esta sistemática habría argumentos tanto para defender una como otra postura. Por un lado, que la utilización ilícita de información de tarjetas o de cheques de viaje en operaciones en perjuicio de terceros constituye una manifestación de fraude informático, dado que la sitúa en el artículo 248.2. Con base en el texto del Proyecto de ley de modificación del Código Penal, de 15 de enero de 2007, así FARALDO CABANA, *Las nuevas tecnologías*, pp. 92 y s. Pero, por otro lado, también cabría defender que tal conducta constituye una nueva modalidad de estafa ajena al fraude informático, dado que se introduce en el artículo 248.2 c) y no en el artículo 248.2 a), junto a éste último.

57 También críticamente v. FERNÁNDEZ TERUELO, *Comentarios a la Reforma Penal de 2010*, p. 281.

58 V. STS de 12 de junio de 2007 (FJ segundo). En cambio, la STS de 16 de marzo de 2009 (FJ 6) mantiene la condena de la instancia inferior por estafa común del artículo 248.1 en un supuesto de *phishing*. También castigando por el artículo 248.2 a) un supuesto de *pharming*, v. la SAP de Madrid de 22 de enero de 2009 y la SAP de Vizcaya de 9 de mayo de 2006, un supuesto de *spyware*.

59 En este sentido se han pronunciado FARALDO CABANA, *Las nuevas tecnologías*, p. 82; CHOCLÁN MONTALVO, *El Cibercrimen*, pp. 76 y s., cambiando la posición mantenida en trabajos anteriores; ORTS BERENGUER y ROIG TORRES, *Delitos informáticos*, p. 67; VELASCO NÚÑEZ, *LLP* (2008), pp. 22 y s. En contra MORALES GARCÍA, *La Reforma Penal de 2010*, pp. 191 y s.

60 Originalmente el Tribunal Supremo calificó tales conductas de robo con fuerza en las cosas por utilización de llave falsa. Cft. esta primera posición en la sentencia de 9 de mayo de 2007.

61 Así en la sentencia de 20 de noviembre de 2001 señala el Tribunal Supremo en su FJ único 3: "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". En el mismo sentido v. las sentencias de 24 de febrero de 2006 (FJ único): "el uso abusivo de tarjetas que permiten operar en un cajero automático puede ser actualmente subsumido bajo el tipo del art. 248.2 CP, dado que tal uso abusivo constituye un «artificio semejante» a una manipulación informática, pues permite lograr un funcionamiento del aparato informático contrario al fin de sus programadores"; y de 30 de mayo de 2009 (FJ tercero), ésta última hace referencia a las dos posturas doctrinales sobre el concepto de manipulación informática. En supuestos similares v. también las sentencias de 17 de diciembre de 2008 (FJ segundo) y de 21 de diciembre de 2004 (FJ segundo), que, sin embargo, en mi opinión constituyen supuestos típicos de fraude por manipulación informática mediante introducción de datos falsos en el sistema, conforme al concepto de manipulación informático defendido mayoritariamente.

62 V. STS de 9 de mayo de 2007 (FJ séptimo): "La identificación a través del numero secreto genera una presunción de uso del sistema por parte de su titular, y por ello, debe incluirse como una modalidad de manipulación informática, a los efectos de aplicar el art. 248.2 el mero hecho de utilizar el numero secreto de otro para identificarse ante el sistema, aunque incluso dicho numero hubiese sido obtenido al

IV

Conforme a lo expuesto en el apartado anterior se puede concluir que esta nueva forma de criminalidad patrimonial consistente en la realización de transferencias bancarias en línea en perjuicio de terceros mediante la utilización no consentida de claves personales de acceso y firma electrónicas puede castigarse adecuadamente a través de la estafa informática prevista en el artículo 248.2 a) del Código Penal, dado que la utilización no consentida de estos datos constituye la manipulación informática o, al menos, el artificio semejante a aquélla, exigidos en el tipo de lo injusto. Esta es la posición que mantienen el Tribunal Supremo y el resto de tribunales inferiores en las escasas sentencias que hay sobre la cuestión y que defiende un sector de nuestra doctrina, al que me sumo. Y es asimismo el tratamiento jurídico penal que está recibiendo en otros países de nuestro entorno como Alemania.

No obstante, de acuerdo con el concepto restringido de manipulación informática defendido por la doctrina mayoritaria de nuestro país desde hace décadas, dichas conductas serían atípicas, de ahí que algún autor haya propuesto la incorporación de nuevos tipos penales basados en la ejecución de operaciones informáticas no autorizadas perjudiciales para el patrimonio de un tercero o en la suplantación de personalidad[63].

margen de cualquier actividad delictiva. En definitiva, identificarse ante el sistema informático mendazmente, introducir datos en el sistema que no se corresponden con la realidad, ha de ser considerado bajo la conducta de manipulación informática o que se refiere el tipo de la estafa del art. 248.2 CP (...) "Esta postura es compartida por aquellos que consideran que en tales casos se están ocultando datos reales e introduciendo datos falsos en el sistema: se oculta la identidad real del operador y se suplanta la del verdadero titular. Tal identificación, a través de la introducción del número secreto obtenido indebidamente, tiene una relevancia o eficacia jurídica que constituye el dato clave para estimar que estamos ante una manipulación informática".

63 Así, FERNÁNDEZ TERUELO, *Cibercrimen*, p. 52. Defendiendo la posición contraria, pero también apoyando la reforma de la estafa informática para recoger expresamente estos supuestos y proponiendo la idea de la suplantación de la personalidad v. VELASCO NÚÑEZ, *LLP* (2008), p. 24.