Estudios Penales y Criminológicos, vol. XXXIV (2014). ISSN 1137-7550: 301-339

RESPUESTA PENAL AL DENOMINADO ROBO DE IDENTIDAD EN LAS CONDUCTAS DE *PHISHING* BANCARIO*

Fátima Flores Mendoza
Profesora Titular de Derecho Penal
Departamento de Disciplinas Jurídicas Básicas
Universidad de La Laguna

Resumen: Este trabajo se ocupa de establecer la responsabilidad penal por la obtención subrepticia de claves y contraseñas bancarias de terceros (datos personales relativos a la identidad) mediante correos electrónicos fraudulentos y programas maliciosos que tiene lugar en los fraudes de banca electrónica, denominados *phishing*. Tales conductas se corresponden a su vez el llamado robo de identidad de otra compleja manifestación criminal, que recibe el mismo nombre. El artículo analizará la adecuación de los delitos contra la intimidad de nuestro Código Penal para casticar estas conductas.
Palabras clave: robo de identidad, intrusismo informático, delitos contra la intimidad, *phishing*, *pharming*, *spyware*

Recibido: julio 2014. Aceptado: octubre 2014

* Este trabajo se ha realizado 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.

Abstract: This article is focused on the criminal liability of the online banking fraud, named phishing, in which the scammers obtain the username and password of the victim (personal identity data) through fraudulent mails and malware. These actions are related with other complex criminal activity, called identity theft. This paper examines the privacy offences of the Spanish Penal Code in order to punish these criminal behaviors.
Keywords: identity theft, hacking, privacy offences, phishing, pharming, spyware

I. Delimitación del objeto de estudio: obtención subrepticia de datos personales relativos a la identidad en el *phishing* bancario

En este trabajo me centraré en la respuesta que ofrece nuestro Código Penal a un nuevo fenómeno criminal denominado *phishing* bancario, término utilizado por doctrina y jurisprudencia para denominar una compleja manifestación criminal de fraude de la banca en línea por la que los delincuentes (*scammers*), sirviéndose de la Red (Internet), acceden subrepticiamente a las claves de acceso y de operaciones bancarias de las víctimas para posteriormente realizar transferencias bancarias en su perjuicio.

Esta nueva manifestación de fraude bancario se desarrolla en tres fases, ejecutadas por sujetos de diferentes nacionalidades, previamente concertados y organizados, que actúan en diferentes estados, y con una alta cualificación tecnológica, lo que dificulta su

persecución. Nos enfrentamos, por tanto, a un nuevo ejemplo de delincuencia organizada, de carácter tecnológico y transnacional[1].

La primera fase tiene por objetivo la obtención ilícita de datos confidenciales para el control de las cuentas bancarias de las víctimas (claves secretas de acceso y de operaciones) a través de Internet y mediante diversas modalidades. La originaria y más frecuente, y que da nombre a todo el fenómeno criminal es la de *phishing* o pesca de los datos a través del correo electrónico (ingeniería social). Esta modalidad consiste en el envío masivo e indiscriminado de correos 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.[2,3].

---

1 Ampliamente sobre la ejecución de estos ataques al patrimonio en nuestro país v. el Auto de la AP de Barcelona, de 23 de octubre de 2009, así como los trabajos de Stuckenberg, C. F.: "Zur Strafbarkeit von *Phishing*", en *ZStW* (118-4), 2006, p. 878 y ss. y Flor, R.: "*Phishing* y delitos relacionados con el fraude de identidad: un *World Wide Problem* en el *World Wide*", en *Robo de identidad y protección de datos*: A. Rallo Lombarte / L. Arroyo Zapatero (Dir.), Cizur Menor, 2010, p. 77 y ss., que lo califica también como "fenómeno criminal complejo" (p. 87).

2 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. Miró Llinares, F.: "La respuesta penal al ciberfraude. Especial atención a la responsabilidad penal de los muleros del *phishing*", en *RECPC* (15-12), 2013, p. 6 y ss. (en línea). Disponible en: http://criminet.ugr.es/recpc (último acceso: 29 de mayo de 2014); Fernández Teruelo, J. G.: *Cibercrimen. Los delitos cometidos a través de Internet*, Madrid, 2007, p. 29 y s.; Velasco Núñez, E.: "Estafa informática y banda organizada. *Phishing, pharming, smishing* y muleros", en *La Ley Penal* (49), 2008, p. 21; el mismo, "Fraudes informáticos en la red: del *phishing* al *pharming*", en *La Ley Penal* (37), 2007, p. 57 y s.; Hansen, D.: *Strafbarkeit des Phishing nach Internetbanking-Legitimationsdaten*, Hamburg, 2007, p. 13 y ss.

3 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

Más sofisticada y, por tanto, más peligrosa es la variante del *pharming*, mediante el uso de los llamados "redirectores". Aquí se utiliza la Red para acceder al servidor DNS (sistema de nombres de dominio) y modificar las direcciones URL e IPs ahí contenidas; al *router* o encaminador del sistema informático de un usuario, modificando la configuración del servidor DNS del sistema; o al propio sistema informático alterando las direcciones URL e IPs contenidas en el archivo *hosts* o alterando la configuración DNS del sistema, dirigiéndolo a un servidor DNS controlado por los atacantes[4] (*pharming* local). Con estas tres modalidades de *pharming* se pretende dirigir a la víctima a páginas electrónicas falsas, creadas expresamente por los delincuentes, en las que aquélla dejara constancia de sus claves de acceso y de operaciones electrónicas[5]. La primera forma de ataque es la menos frecuente por las medidas de protección que tienen los servidores DNS. No obstante, sus efectos serían más graves, pues al modificar una URL o dirección IP de, por ejemplo, una entidad bancaria contenida en un servidor o servidores, todos los usuarios que quieran acceder a esa página son redirigidos a una

---

quedarían recogidas actualmente en el nuevo tipo del art. 399 bis CP, relativo a la falsificación de tarjetas bancarias, que entraría en concurso de leyes con la nueva modalidad de estafa del art. 248.2 c) CP, 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.

4 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.

5 V. más ampliamente, Miró Llinares, "La respuesta penal al ciberfraude", p. 10; Faraldo Cabana, P.: *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Valencia, 2009, p. 91; Fernández Teruelo, *Cibercrimen*, p. 30. De forma similar Velasco Núñez, "Estafa informática y banda organizada", p. 21; el mismo, "Fraudes informáticos en la red: del *phishing* al *pharming*", p. 59 y s.

página falsa diseñada por los delincuentes (*scammers*), que crean su propia granja (*farm*, *pharming*) de víctimas.

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 (*man-in-the-middle*). 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[6]. 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*)[7,8].

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[9]. 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

---

6 V. más ampliamente, Miró Llinares, "La respuesta penal al ciberfraude", p. 10; Fernández Teruelo, *Cibercrimen*, p. 28 y s.

7 Sobre nuevas manifestaciones de *phishing* v. Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 87.

8 Sobre otras formas de acceso a la información personal v. el trabajo de Salvadori, I.: "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", en *Robo de identidad y protección de datos*: A. Rallo Lombarte / L. Arroyo Zapatero (Dir.), Cizur Menor, 2010, p. 227 y ss.

9 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.

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[10]. En nuestro país en 2013 los procesos penales por *phishing* (en sentido amplio) han aumentado en un 30% respecto del año anterior[11] y según informa el Instituto Nacional de Tecnologías de la Comunicación (INTECO) en uno de sus informes, el fraude bancario a través de la variante de correos electrónicos (*phishing*) sigue siendo la más habitual[12].

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[13], lo que permite hablar de delincuencia organizada,

---

10 Tal y como informa en su trabajo Stuckenberg, "Zur Strafbarkeit von *Phishing*", p. 878 y ss. Sobre el volumen del fraude en nuestro país v. R. Mata y Martín, R.: "El robo de identidad: ¿una figura necesaria?", en *Robo de identidad y protección de datos*: A. Rallo Lombarte / L. Arroyo Zapatero (Dir.), Cizur Menor, 2010, p. 208 y s. V. asimismo los datos aportados por Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 84 y ss.; Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 221. y s.

11 V. Gómez Iniesta, D.: "Estafa y blanqueo de dinero a través de Internet", en *La Ley* (105), 2013, p. 1 y s. (en línea). Disponible en http://revistas.laley.es/Content/Documento.aspx?params=H4sIAAA (último acceso: 29 de mayo de 2014).

12 V.http://www.inteco.es/CERT/guias_estudios/Estudios/Estudio_fraude_1C2012 (último acceso: 1 de julio de 2014).

13 En este sentido v. Velasco Núñez, "Fraudes informático en la red: del *phishing* al *pharming*", p. 62; el mismo, "Estafa informática y banda organizada", p.

altamente cualificada e internacional[14]. 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[15]. 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 del art. 570 bis CP, introducidos por la LO 5/2010, de 22 de junio, por la que se modifica el Código Penal[16]. Conforme al art. 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 art. 515.1º CP, con el que entraría en concurso de leyes [17,18]. El Código Penal resuelve este

21. También resulta muy ilustrativo el Auto de la AP Barcelona, de 23 de octubre de 2009.

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

15 Sobre la dificultad para determinar el lugar de comisión de los delitos cometidos a través de Internet y 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 / F. G. Sánchez Lázaro (Eds.), Granada, 2010, p. 331-345.

16 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.

17 La organización criminal parece más adecuada en estos casos que la de asociación ilícita del art. 515 CP, definida por la doctrina y jurisprudencia como la unión de un mínimo dos o tres personas para la realización de alguno

concurso a favor de la organización criminal con base en el principio de alternatividad (art. 570 quáter 2). El delito del art. 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 quáter 3 CP).

A este delito habría que añadir la responsabilidad penal por los atentados contra el patrimonio y el orden socioeconómico de la segunda y tercera fases, respectivamente, y, en su caso, los atentados a la intimidad, al patrimonio y a la fe pública, de la primera. En un segundo momento, tras la obtención subrepticia de las claves bancarias, las mismas son utilizadas por estos u otros sujetos (que las adquieren de los anteriores) para realizar con ánimo de lucro transferencias en línea no consentidas por sus

---

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. Sánchez García de Paz, I.: *Comentarios al Código Penal*: M. Gómez Tomillo (Dir.), 2ª ed., Valladolid, 2011, p. 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 dificultad para diferenciarlas v. Martell Pérez-Alcalde, C. / Quintero García, D.: "*De las organizaciones y grupos criminales*", en *La Reforma Penal de 2010: Análisis y Comentarios*: G. Quintero Olivares (Dir.), Cizur Menor, 2010, p. 360 y s. También v. Velasco Núñez, E.: "Delitos informáticos realizados en actuación organizada", en *Diario La Ley* (7743), 2011, p. 3 (en línea). Disponible en: http://www.laleydigital.es (último acceso: 6 de agosto de 2013). Este autor considera que cuando la finalidad de la agrupación es delictiva concurren los tipos del Capítulo IV del Título XXII del Libro II del Código Penal. Y antes de la reforma v. asimismo el estudio y propuestas de Brandariz García, J. A.: "Asociaciones y organizaciones criminales. Las disfunciones del art. 515.1º CP y la nueva reforma penal", en *La adecuación del Derecho Penal Español al ordenamiento de la Unión Europea. La Política Criminal Europea*: F. J. Álvarez García (Dir.), Valencia, 2009, p. 725 y ss.

18 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.

titulares, con el consiguiente perjuicio patrimonial de terceros. Esta conducta constituye en mi opinión una estafa informática, castigada en el art. 248.2 a) CP[19]. Por otro lado, esta manifestación criminal se completa con la actuación de los denominados muleros, que daría lugar a una responsabilidad por blanqueo de capitales en concurso real con una estafa informática, esta última a título de participación[20,21]. Asimismo, los autores de la estafa informática podrían responder como autores mediatos o inductores del blanqueo de capitales llevado a cabo por los intermediarios o muleros.

En este trabajo me ocuparé de la respuesta que ofrece nuestro Código Penal a la conducta de acceso fraudulento o subrepticio a través de la Red a las claves bancarias de las víctimas, mediante las técnicas de *phishing*, *pharming* y *spyware*, ya mencionadas. El objeto de esta investigación será, por tanto, determinar si estas conductas se pueden reconducir a los delitos contra la intimidad o si, por el contrario, son necesarios nuevos tipos de lo injusto para castigarlas.

Hasta el momento las excepcionales resoluciones judiciales que han conocido de casos de acceso ilícito de datos personales bancarios efectuados por los mismos sujetos que posteriormente cometen el fraude informático no han condenado y ni siquiera entrado al enjuiciamiento de esta primera fase como un atentado contra la intimidad[22]. Las razones pueden hallarse en que, como ya se ha indicado, son ejecutadas por organizaciones criminales cuyos miembros cuentan con una alta cualificación tecnológica,

19 Sobre el alcance de esta figura delictiva v. mi trabajo "Nuevas formas de criminalidad patrimonial a través de Internet", en *Revista Penal* (29), 2012, p. 75-86.

20 De la responsabilidad penal de estos sujetos me he ocupado en: "La responsabilidad penal del denominado mulero o *phisher-mule* en los fraudes de banca electrónica", en *Cuadernos de Política Criminal* (110), 2013, p. 155-187.

21 Del tratamiento jurídico-penal de esta manifestación criminal en Alemania, Italia y Estados Unidos da cuenta Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 87 y ss.

22 Como así ocurre en la SAP de Lérida, de 2 de septiembre de 2011, que recoge un supuesto de *phishing*.

y en que operan desde el extranjero, respondiendo en nuestro país únicamente los denominados intermediarios o muleros por su contribución en las fases posteriores.

Estas conductas propias del *phishing* (en sentido amplio) se corresponden con el mal denominado robo de identidad, que consiste en la obtención de datos personales reservados o secretos relativos a la identidad de un individuo. Pero el *identity theft* también es utilizado en la comisión de otros fraudes (apertura de cuentas bancarias, utilización de tarjetas de crédito, solicitud de préstamos, comercio electrónico, etc.) y otras conductas delictivas (falsedades, blanqueo de capitales, sabotaje informático, etc.)[23].

El *identity theft* (cuya traducción literal sería hurto de identidad y no robo de identidad[24]) forma parte, a su vez, de otro fenómeno criminal más amplio, denominado *identity related crime* o *identity theft* en sentido amplio[25,26], que se divide en dos o tres fases[27]. La primera se corresponde con las conductas de hurto de identidad en sentido estricto. En ella los delincuentes obtienen (*se apoderan de*) los datos reservados relativos a la identidad de una persona física, viva o muerta, o jurídica o agrupación o entidad

23 V. Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 224.

24 El robo de identidad se correspondería con la expresión *identiy robbery*. De la denominación recibida en otras legislaciones informa Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 223 y ss.

25 V. al respecto Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 80.

26 De la respuesta legislativa en Estados Unidos a esta compleja figura da cuenta Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 228 y ss. En cambio en Europa no contamos con una normativa equivalente. Sobre las iniciativas legislativas en el ámbito de la Unión Europea v. Muñoz de Morales Romero, M.: "¿De la nada al todo?: La importación del robo de identidad por la Unión Europea", en *Robo de identidad y protección de datos*: A. Rallo Lombarte / L. Arroyo Zapatero (Dir.), Cizur Menor, 2010, p. 155 y s.

27 Así, Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 226 y s.

sin personalidad jurídica[28]. Estos datos pueden ser de carácter electrónico, de ahí que se hable de identidad electrónica o digital[29]. En la segunda fase tiene lugar la suplantación de la identidad, esto es, la utilización de los datos personales ajenos con fines ilícitos, sean estos delictivos o no, que se conoce con el nombre de *identity fraud* o *identity abuse*[30,31]. Entre ambas etapas puede existir una tercera en la que se produce la venta o tráfico de los datos de identidad a otros sujetos u organizaciones criminales[32].

En este trabajo tan sólo me interesa analizar la primera fase de esta manifestación criminal, esto es, el *identity theft* o hurto de identidad, que se corresponde a su vez con la primera etapa del *phishing*. De la suplantación de identidad ajena con fines ilícitos (*identity fraud* o *identity abuse*) y de la necesidad político criminal de castigarla de forma autónoma, dada la insuficiencia de la usurpación de estado civil del art. 401 CP[33], o conjuntamente con la primera etapa, me ocuparé en otro lugar[34,35].

---

28 Así lo considera Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 83.

29 Al respecto v. Mata y Martín, "El robo de identidad: ¿una figura necesaria?", p. 203.

30 Así, Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 80.

31 Esto es lo que ocurre también en el *phishing* bancario, en la que determinados miembros de la organización criminal llevan a cabo las transferencias patrimoniales no consentidas a través de la banca electrónica, mediante la suplantación de la identidad (electrónica) de los titulares de las cuentas corrientes. En estos casos la suplantación de la identidad electrónica (*identity fraud* o *identity abuse*) constituye la manipulación informática o artificio semejante de la estafa informática del art. 248.2 a) CP. V. sobre estos conceptos mi trabajo "Nuevas formas de criminalidad patrimonial a través de Internet", en *Revista Penal* (29), 2012, p. 82 y ss.

32 Sobre ella v. Muñoz de Morales Romero, "¿De la nada al todo?: La importación del robo de identidad por la Unión Europea", p. 158 n. 151. Esta conducta encontraría respuesta penal a través del tipo agravado del art. 197.4 CP, que sanciona la revelación, difusión o cesión a terceros de tales datos personales obtenidos ilícitamente.

33 Así, v. Mata y Martín, "El robo de identidad: ¿una figura necesaria?", p. 214 y s. En el mismo sentido v. Galán Muñoz, A.: "El robo de identidad: aproximación a una nueva y difusa conducta delictiva", en *Robo de identidad*

En nuestro país el *identiy theft* ha recibido diversas denominaciones por parte de la doctrina: robo[36], hurto[37], sustracción[38] o usurpación de identidad[39], aunque la más conocida es la de robo de identidad. Sin embargo, esto términos resultan inapropiados para designar esta realidad[40]. En primer lugar, porque, como se ha señalado, la denominación original debería traducirse por hurto de identidad. Y en segundo lugar, porque estas denominaciones se identifican con los delitos de apoderamiento, propios de los delitos contra el patrimonio, en los que tiene lugar la desposesión del objeto material al sujeto pasivo (la cosa mueble ajena), con el consiguiente desplazamiento de la misma a manos del sujeto

---

y protección de datos: A. Rallo Lombarte / L. Arroyo Zapatero (Dir.), Cizur Menor, 2010, p. 171. Admite la posibilidad de apreciar el delito de usurpación de funciones públicas del art. 402 CP Miró Llinares, "La respuesta penal al ciberfraude", p. 19.

34 A favor de su introducción al Código Penal entre las falsedades personales del Título XVIII v. Mata y Martín, "El robo de identidad: ¿una figura necesaria?", p. 220; también a favor de su incriminación Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 78 y ss. Nieto Martín propone que el bien jurídico protegido en estas conductas sea "la confianza en los medios de pago del comercio electrónico". V. Nieto Martín, A.: "Identity theft and internacional criminal policy: manufacturing consent", en *Cahiers de défense sociale: bulletin de la Societé International de Défense Sociale pour une Politique Criminelle Humaniste* (36), 2009-2010, p. 30 (en línea). Disponible en: http://dialnet.unirioja.es (último acceso: 9 de julio de 2014).

35 En Estados Unidos se castiga como hurto de identidad la transferencia, posesión o utilización sin autorización de datos identificativos de un tercero con intención de cometer, intentar o favorecer cualquier actividad ilícita. La OCDE define esta figura de forma similar pero incluye las conductas de obtención ilícita de datos personales ajenos. Al respecto v. Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 225 y 228 y ss.

36 Utiliza esta denominación Mata y Martín, "El robo de identidad: ¿una figura necesaria?", p. 202.

37 Así, Flor, "*Phishing* y delitos relacionados con el fraude de identidad", p. 83; Salvadori, "La lucha contra el hurto de identidad: las diferentes perspectivas legislativas", p. 221.

38 V. Gómez Iniesta, "Estafa y blanqueo de dinero a través de Internet", p. 2.

39 Así, Galán Muñoz, "El robo de identidad: aproximación a una nueva y difusa conducta delictiva", p. 169.

40 También lo considera así Galán Muñoz, v. ult. lug. cit.

activo. En cambio, en estas otras conductas el objeto material no es una cosa mueble, sino paradójicamente un objeto inmaterial, datos relativos a la identidad de una persona. Y, por tanto, no es necesario que exista una desposesión o desplazamiento de estos. En este fenómeno criminal tan sólo es necesario que los delincuentes accedan, obtengan o se hagan con tales datos, sin que sea preciso que su titular los pierda. Es más, ni siquiera se requiere que el delincuente se haga con una copia de aquellos, aunque sea esto lo más frecuente, pues bastaría que los memorizara una vez haya accedido a ellos. Por ello considero más adecuada la referencia *obtención subrepticia a los datos personales relativos a la identidad*, que aunque menos impactante, es más precisa y evita confusiones[41]. No obstante, no habría inconveniente en utilizar los términos apoderamiento o sustracción de datos relativos a la identidad, siempre que se interpretasen de forma espiritualizada de acuerdo con su objeto material[42].

II. Respuesta penal a la obtención subrepticia de claves personales ajenas conforme a los delitos contra la intimidad

La intimidad personal, reconocida como derecho fundamental en el art. 18.1 CE, constituye el bien jurídico de los delitos del Título X, Capítulo Primero del Código Penal. Su objeto es el de garantizar a su titular un espacio privado destinado al desarrollo de su personalidad a salvo del conocimiento e intromisiones ajenas[43]. De este reconocimiento se deriva la facultad de su

41 Como así ha sucedido con el alcance del apoderamiento de los correos electrónicos de otro para descubrir sus secretos o vulnerar su intimidad, del art. 197.1 CP. Sobre la discusión doctrinal al respecto v. el apartado II.5.

42 Como así se ha interpretado la acción típica de apoderamiento de correos electrónicos ajenos del mencionado art. 197.1 CP. V. al respecto Romeo Casabona, C. M.: *Los delitos de descubrimiento y revelación de secretos*, Valencia, 2004, p. 83 y ss.

43 V. González Rus, J. L.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)", en *Sistema de Derecho Penal Español. Parte Especial*: L Morillas Cueva (Dir.), Madrid, 2011, p. 298 y ss.; Anarte Borrallo, E. / Doval Pais, A.: "Delitos contra la intimidad, el

titular de excluir a los terceros de este espacio personal privado reconocido, cuyo alcance será determinado por el propio titular (dimensión negativa)[44]. Junto a ella se reconoce una facultad de autodeterminación informativa o derecho al control de los datos personales (art. 18.4 CE), que para un sector constituye la dimensión positiva de la intimidad[45] y, por tanto, del mismo bien jurídico, mientras que para otro representa un bien jurídico independiente (libertad informática)[46].

Las figuras delictivas del art. 197.1 CP, que analizaremos a continuación, se presentan como delitos de intención, que persiguen el descubrimiento de los secretos ajenos y la vulneración de su intimidad (elemento subjetivo de lo injusto). Así, para unos el secreto debe ser entendido como los datos o hechos que por voluntad de la persona a la que conciernen quedan reservados al conocimiento de unos pocos y ocultos al conocimiento de la mayoría[47]. Para otros, en cambio, no basta con la voluntad del titular

---

derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", en *Derecho Penal. Parte Especial* (*Vol. I)*: J. Boix Reig (Dir.), Madrid, 2010, p. 443.

44 Así, González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 299; Romeo Casabona, C. M.: "Del descubrimiento y revelación de secretos", en *Comentarios al Código Penal. Parte Especial. II*: J. L. Díez Ripollés / C. M. Romeo Casabona (Coords.), Valencia, 2004, p. 717. Sin embargo, para otros autores el ámbito de protección de la intimidad deberá ser determinado de acuerdo con criterios de adecuación social. En este sentido v. Morales Prats, F.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Comentarios a la Parte Especial del Derecho Penal*: G. Quintero Olivares (Dir.), 9ª ed., Cizur Menor, 2011, p. 457 y s.; Orts Berenguer, E. / Roig Torres, M.: *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001, p. 21.

45 Así, Jorge Barreiro, A.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Memento Práctico Penal*, Madrid, 2011, n.m. 9856; González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 299.

46 V. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 40 y ss.

47 De forma similar, Romeo Casabona, *Comentarios al Código Penal.*, p. 717. Así también lo entienden nuestros tribunales, que admiten bajo el concepto de secreto la documentación bancaria o económica y la correspondencia

de mantener reservado el dato o información, sino que el secreto deberá ser delimitado conforme a criterios de adecuación social, como se ha señalado[48]. Sea delimitada la intimidad de una u otra forma, no veo obstáculos para afirmar que las claves de acceso y de operaciones bancarias, objetivo inmediato de las conductas de *phishing*, pueden ser consideradas información personal reservada o privada, y, por tanto, quedar cubiertas por la intimidad[49].

1. Por el delito de intrusismo informático

De entre las diferentes conductas delictivas previstas en el Capítulo Primero del Descubrimiento y revelación de secretos, del Título X de los Delitos contra la intimidad del Código Penal, las técnicas de *pharming* y *spyware* se acercan a los comportamientos de *hacking* o intrusismo informático del art. 197.3[50].

Siguiendo el modelo italiano y francés este precepto incorpora un tipo alternativo que recuerda al allanamiento de morada. Así, prohíbe tanto el acceso ilícito a datos o programas de un sistema informático o de una parte del mismo, vulnerando

---

bancaria. V. al respecto Tomás Valiente Lanuza, C.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Comentarios al Código Penal*: M. Gómez Tomillo (Dir.), 2ª ed., Valladolid, 2011, p. 794 y s. Cft. Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 458.

48 Orts Berenguer / Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 24; Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 458.

49 Cuestiona su consideración de datos íntimos o secretos Miró Llinares, "La respuesta penal al ciberfraude", p. 21.

50 En relación con la discusión doctrinal previa sobre su denominación, contenido y necesidad de incriminación v. Rueda Martín, M. A.: "Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales", en *La adaptación del Derecho Penal al desarrollo social y tecnológico*: C. M. Romeo Casabona / F. G. Sánchez Lázaro (Eds.), Granada, 2010; p. 347 y ss.; Carrasco Andrino, M. M.: "El acceso ilícito a un sistema informático", en *La adecuación del Derecho penal español al ordenamiento de la Unión Europea*: J. Álvarez García, (Coord.), Valencia, 2009, p. 356 y ss.; Matellanes Rodríguez, N.: "Vías de tipificación del acceso ilegal a los sistemas informáticos (I)", en *Revista Penal* (22), 2008, p. 50 y ss.

las medidas de seguridad de aquel (comportamiento activo), como la permanencia no consentida en dicho sistema informático (comportamiento omisivo)[51,52].

El bien jurídico es objeto de discusión por parte de la doctrina, que se divide entre los partidarios de la intimidad[53] y

51 El art. 197.3 establece: El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

52 Este nuevo precepto, introducido por la LO 5/2010, de 22 de junio, de reforma del Código Penal, trae causa de la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información y del Convenio del Consejo de Europa sobre Cibercriminalidad, firmado en Budapest el 23 de noviembre de 2001, y ratificado por España el 3 de junio de 2010. El Proyecto de Código Penal de 2009, siguiendo la propuesta de la directiva europea, incorpora al precepto el comportamiento omisivo, que no se hallaba en la redacción original del Anteproyecto de reforma de Código Penal de 2008, ni en el Proyecto de 15 de enero de 2007. Sobre su justificación y las propuestas jurídicas internacionales, de derecho comparado y nacionales v. Carrasco Andrino, "El acceso ilícito a un sistema informático", p. 342 y ss.; Matellanes Rodríguez, "Vías de tipificación del acceso ilegal a los sistemas informáticos (I)", p. 56 y ss.

53 Consideran que el precepto protege la intimidad a través de denominado "domicilio informático" Morales García, O.: "Delincuencia informática: instrusismo, sabotaje informático y uso ilícito de tarjetas", en *La reforma penal de 2010: análisis y comentarios*: G. Quintero Olivares (Dir.), Cizur Menor, 2010, p. 185 y s.; Alonso Escamilla, A.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en *Delitos y faltas. La parte especial del Derecho Penal*: C. Lamarca Pérez (Coord.), 2ª ed., Madrid, 2013, p. 219; Ragués i Vallès, R. / Robles Planas, R.: "La reforma de los delitos informáticos: incriminación de los ataques a sistemas de información", en *El nuevo Código Penal. Comentarios a la reforma*: J. M. Silva Sánchez (Dir.), Madrid, 2012, p. 371; Corcoy Bidasolo, M. / Mir Puig, S.: "Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio", en *Comentarios al Código Penal. Reforma LO 5/2010*: M. Corcoy Bidasolo / S. Mir Puig (Dirs.), Valencia, 2011, p. 469. Y ya antes, con ocasión del tenor literal del art. 197.3 del Proyecto de Reforma del Código Penal de 2007, v. Matellanes Rodríguez, N.: "Vías de tipificación del acceso ilegal a los sistemas informáticos (II)", en *Revista Penal* (23), 2009, p. 63 y ss., especialmente p. 67.

los defensores de la seguridad jurídica[54,55], criticando esta última posición la situación del precepto entre los delitos contra la intimidad personal[56].

Mayoritariamente se mantiene que esta nueva figura no constituye un delito de intención, pues el precepto no requiere el ánimo de vulnerar la intimidad ajena[57], pero sí exigiría la denominada *introducción lógica*, esto es, la necesidad de que el intruso acceda no sólo al sistema informático, sino también a sus datos o programas informáticos[58]. Por otro lado, a diferencia de lo

---

54 Así, Muñoz Conde, F.: *Derecho Penal. Parte Especial*, 19ª ed., Valencia, 2013, p. 261; Tomás Valiente Lanuza, *Comentarios al Código Penal*, p. 802; Carrasco Andrino, M. M.: "El delito de acceso ilícito a los sistemas informáticos", en *Comentarios a la Reforma Penal de 2010*: F. J. Álvarez García / J. L. González Cussac (Dirs.), Valencia, 2010, p. 250; la misma, "El acceso ilícito a un sistema informático", p. 255, haciendo referencia al Proyecto de Ley Orgánica de 2007. También críticamente, pero considerando el bien jurídico debe ser la seguridad de los sistemas informáticos orientada a la protección de la intimidad informática, v. Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 483.

55 Planteando ambas posibilidades tanto la intimidad como la seguridad jurídica de los sistemas informáticos, v. Carbonell Mateu, J. C. / González Cussac, J. L.: *Derecho Penal. Parte Especial*: T. S. Vives Antón y otros, 3ª ed., Valencia, 2010, p. 325.

56 Sobre la discusión previa a su incorporación al Código Penal v. Matellanes Rodríguez, "Vías de tipificación del acceso ilegal a los sistemas informáticos (I)", p. 64 y ss.

57 En este sentido v. Corcoy Bidasolo / Mir Puig, *Comentarios al Código Penal. Reforma LO 5/2010*, p. 469; Morales García, "Delincuencia informática: instrusismo, sabotaje informático y uso ilícito de tarjetas", p. 185; Carrasco Andrino, "El acceso ilícito a un sistema informático", p. 361, admitiendo en el tipo el denominado *hacking* blanco. En contra Carbonell Mateu / González Cussac, *Derecho Penal. Parte Especial*, p. 325.

58 Como ha puesto de manifiesto Carrasco Andrino, "El acceso ilícito a un sistema informático", p. 357 y s. y 361 y s., la consideración de que el precepto recoge un supuesto de introducción lógica no tiene que ver con la necesidad de concurrencia de un elemento subjetivo, sino con la exigencia de que se acceda a los datos o programas alojados en un sistema informático o parte de él. En el mismo sentido v. Matellanes Rodríguez, "Vías de tipificación del acceso ilegal a los sistemas informáticos (II)", p. 62 y s., para la que el intrusismo del art. 197.3 CP sigue el modelo del § 202a StGB; y también en "Vías de tipificación del acceso ilegal a los sistemas informáticos (I)", p.

establecido en los preceptos anteriores (art. 197.1 y 197.2 CP) estos datos no tienen que ser datos personales secretos o reservados[59].

Configurado así el tipo de lo injusto, considero que tanto el *pharming* como el *spyware* consisten en un acceso no consentido al sistema informático de un tercero llevado a cabo de forma remota a través de la Red, modificando las direcciones IPs o configuración DNS de un sistema informático, en el primero, e introduciendo programas espía en el sistema, en el segundo[60]. En la mayoría, si no en todos los casos, tales conductas se realizarán vulnerando las medidas de seguridad del sistema o de los propios datos o programas[61], por mínimas que éstas sean (cortafuegos o *firewalls*, contraseñas de encendido del sistema, de acceso al sistema, al teclado, de bloqueo del sistema, dispositivos de

62. Este elemento típico impediría el castigo del *hacking* puro a través del art. 197.3 CP. Así, Matellanes Rodríguez, "Vías de tipificación del acceso ilegal a los sistemas informáticos (II)", 2009, p. 54.

59 Así, Corcoy Bidasolo / Mir Puig, *Comentarios al Código Penal. Reforma LO 5/201*, p. 469; Carbonell Mateu / González Cussac, *Derecho Penal. Parte Especial*, p. 325. Más ampliamente Matellanes Rodríguez, "Vías de tipificación del acceso ilegal a los sistemas informáticos (II)", p. 63, que defiende que los datos pueden ser de carácter profesional, laboral, económico, etc. En cambio, para Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 484, sería necesario que se accediese a datos o programas que potencialmente pudiesen albergar datos personales, dada la situación sistemática del precepto.

60 No así en el *phishing*, en el que es la propia víctima la que proporciona a los defraudadores las claves de acceso y de operaciones bancarias. En el mismo sentido en la doctrina alemana v. Hilgendorf, E.: *Leipziger Kommentar StGB* 12. Auf., Berlin, 2010, § 202a n.m. 17; Kinhäuser, U.: *Strafgesetzbuch. Lehr- und Praxiskommentar,* 4. Auf., Baden-Baden, 2010, § 202a n.m. 5, con ulteriores referencias bibliográficas; Graf, J. P.: "Phishing derzeit nicht generell strafbar!", en *NStZ* (3), 2007, p. 131; Stuckenberg, "Zur Strafbarkeit von Phishing", p. 884 y s. De otra opinión, v. Gercke, M.: "Die Strafbarkeit von Phishing und Identitätsdiebstahl", en *Computer und Recht* (8), 2005, p. 611 y s.; Knupfer, J.: "Phishing for money", en *MMR* (10), 2004, p. 642.

61 Como bien apunta Matellanes Rodríguez, "Vías de tipificación del acceso ilegal a los sistemas informáticos (II) ", p. 65.

reconocimiento de voz, criptografía de datos, etc.)[62]. Siendo así, ambas técnicas darían lugar al delito de intrusismo informático del 197.3 CP, en su modalidad activa[63]. No obstante, el desvalor de lo injusto de las mismas no quedaría cubierto con este delito, que no exige que el sujeto activo se apodere de datos personales o los altere[64].

Cabe plantearse, sin embargo, si este tipo concurriría en las tres variantes de *pharming* señaladas más arriba. No cabe duda que la modalidad de *pharming* local, en la que el sujeto activo accede al sistema informático del usuario, integraría el delito de intrusismo informático, si concurriesen el resto de elementos del tipo. Más dudas plantean las otras modalidades en las que el autor altera la configuración DNS o las direcciones IP accediendo bien al *router* del sistema informático del usuario, bien al servidor DNS.

---

62 De acuerdo con el tenor literal entiendo que las medidas de seguridad abarcan no solo las establecidas para acceder al sistema informático en su conjunto, sino también a aquellas otras que impiden el acceso a una parte del mismo (teclado, disco duro externo, etc.), o específicamente a los datos (o programas informáticos). En el mismo sentido Carrasco Andrino, "El acceso ilícito a un sistema informático", p. 358; Carbonell Mateu / González Cussac, *Derecho Penal. Parte Especial*, p. 325.

63 En el mismo sentido críticamente v. Fernández Teruelo, J. G.: "Estafas", en *Comentarios a la Reforma Penal de 2010*: F.J. Álvarez García / J.L. González Cussac (Dirs.), Valencia, 2010, p. 278. Más ampliamente sobre estos programas (*keyloggers, sniffers, crackers*) ult. lug. cit. En relación con el *spyware*, v. también Carrasco Andrino, "El delito de acceso ilícito a los sistemas informáticos", p. 253. Así también Miró Llinares, "La respuesta penal al ciberfraude", p. 21. En la doctrina alemana v. al respecto Hansen, *Strafbarkeit des Phishing nach Internetbanking-Legitimationsdaten*, p. 139 y ss. (150); y señalando las insuficiencias del StGB alemán v. Goeckenjan, I.: "Auswierkungen des 41. des Strafrechtsänderungsgesetzes auf die Strafbarkeit des Phishing", en *Wistra* (2), 2009, p. 50 y ss.; Stuckenberg, "Zur Strafbarkeit von Phishing", p. 884; Popp, A.: "Phishing, Pharming und das Strafrecht", en *MMR* (2), 2006, p. 85; el mismo, "Von Datendieben und Betrügern zur Strafbarkeit des sogennanten Phishing", en *NJW* (49), 2004, p. 3518.

64 De ahí que sea necesario analizar la posibilidad de que otro delito contra la intimidad pueda abarcar toda la gravedad de lo injusto de estas conductas.

En el primer supuesto la respuesta dependerá de si este dispositivo forma parte del sistema informático o no. Entiendo que una interpretación teleológica del precepto nos llevaría a considerarlo como parte del sistema informático, conforme al concepto amplio propuesto en el art. 1 de la DM 2205/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información y el art. 1 del Convenio sobre Cibercriminalidad del Consejo de Europa, de 23 de noviembre de 2001[65].

El segundo supuesto constituiría asimismo un acceso no consentido a datos o programas de un sistema informático (servidor), con la única particularidad de que en esta ocasión, la titularidad correspondería en la mayoría de los supuestos a una persona jurídica. En tal caso el tipo de lo injusto aplicable debería ser el del art. 200 CP, atendiendo al principio de especialidad. Pero en este la conducta típica no consistiría en acceder sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo vulnerando las medidas de seguridad, sino en descubrir datos reservados de la persona jurídica sin el consentimiento de sus representantes[66]. Siguiendo a un sector de la doctrina considero que el bien jurídico protegido por el precepto es la confidencialidad de los datos reservados de las personas jurídicas y no la intimidad de las personas físicas relacionadas con aquellas[67]. Y, por otro lado, entiendo que las

65 El citado artículo define al sistema informático como: "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento". En contra Carrasco Andrino, "El acceso ilícito a un sistema informático", p. 360, que entiende que el acceso al *router* a través de su clave de acceso no da lugar al tipo del art. 197.3 puesto que no se accede a datos o programas contenidos en un sistema informático, sino en todo caso a datos enviados o recibidos.

66 Planteando esta posibilidad v. Mata y Martín, "El robo de identidad: ¿una figura necesaria?", p. 214.

67 Sobre el debate planteado en la doctrina y defendiendo esta posición v. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 210; Rueda Martín, M. A.: *Protección penal de la intimidad personal e infor-*

direcciones IP a las que acceden los delincuentes, y posteriormente modifican también sin autorización, constituirían datos reservados de la persona jurídica (entidad bancaria titular de la IP o dominio), de la misma forma que lo son respecto de una persona física, con independencia de donde se hallen alojados (servidor DNS de otra persona jurídica). Así lo han entendido la Agencia Española de Protección de Datos[68] y un sector de la doctrina[69], aunque en relación con las IPs atribuidas a personas físicas, posición que no ha sido seguida, sin embargo, por el Tribunal Supremo[70].

---

mática. Los delitos descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal, Barcelona, 2004, p. 166 y ss., 174 y ss., 182 y s.; Gómez Navajas, J.: *La protección de los datos personales*, Cizur Menor, 2005, p. 133 y 147.

68 V. al respecto el informe 327/2003, de 12 de septiembre, cit. por Lloria García, P.: "El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de Internet. Algunas consideraciones", en *La protección jurídica de la intimidad*: J. Boix Reig (Dir.), Madrid, 2010, p. 191 y ss.

69 Sobre la protección de las IPs en relación con el intercambio de archivos P2P, Lloria García, "El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de Internet", p. 179 y ss., considera que estas direcciones son datos personales protegidos por el art. 18.3 CE, que garantiza el derecho fundamental al secreto de todo tipo de comunicaciones, incluidas las electrónicas, su contenido, cualquiera que este sea, así como los aspectos externos de la misma (interlocutores, fecha, duración, situación, etc.). Apoya esta opinión en la jurisprudencia del Tribunal Constitucional (SSTC 123/2002, de 20 de mayo y 281/2006, de 9 de octubre y 230/2007) y en la sentencia del TJCE de 29 de enero de 2008 (TJCE\2008\11, Gran Sala, Caso Promusicae), que mantiene que las direcciones IPs son datos personales cubiertos por la intimidad: "Una dirección IP cumple la misma función que un número de teléfono: permite identificar a la persona que realiza la comunicación y, por lo tanto, es un dato que debe quedar protegido". En el mismo sentido se ha pronunciado Guerrero Picó, M. C.: *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Cizur Menor, 2006, p. 416 y ss., para la que la dirección IP (al igual que el correo electrónico) es un dato personal si en unión de otros datos identifica a la persona. En este sentido informa que las direcciones IP pueden ser dinámicas o fijas; las primeras permitirían reconocer al proveedor de acceso, mientras que la segunda posibilitaría acceder asimismo al ordenador y a partir de él al usuario.

70 V. las STS de 9 de mayo de 2008 (f.j. 9) y STS de 28 de mayo de 2008 (f.j. 2), citadas por Lloria García, "El secreto de las comunicaciones: su

Asimismo este será el tipo a aplicar cuando las claves bancarias obtenidas subrepticiamente por medio del *phishing*, *pharming* o *spyware* correspondan a una persona jurídica.

En el improbable supuesto de que las conductas de *pharming* o *spyware* pudieran realizarse sin vulnerar las medidas de seguridad del sistema informático no cabría apreciar el tipo activo de intrusismo del art. 197.3 CP, pero tampoco su modalidad omisiva. A pesar de que el tenor literal no lo exige expresamente, se ha interpretado mayoritariamente que la permanencia no autorizada en un sistema informático se reduce a los casos de acceso inicial lícito, en los que el sujeto contó con la oportuna autorización que posteriormente expira o se revoca[71].

2. Por el delito de interceptación de las telecomunicaciones

Asimismo la modalidad de *spyware* daría lugar a la conducta de interceptación de las comunicaciones del art. 197.1 CP. El citado precepto prohíbe la interceptación de las comunicaciones ajenas llevadas a cabo sin consentimiento y con la finalidad de vulnerar su intimidad o descubrir sus secretos. Se protege así el secreto de las comunicaciones reconocido en el art. 18.3 CE[72].

---

interpretación en el ámbito de los delitos cometidos a través de Internet", p. 179 y ss. Esta autora señala que en ellas el Tribunal Supremo mantiene que las direcciones IPs son públicas y que de forma aislada no permiten determinar la identidad del usuario, tan solo la titularidad del sistema informático, por lo que no pueden quedar amparadas por el derecho fundamental del art. 18.3 CE.

71 Así, Carbonell Mateu / González Cussac, *Derecho Penal. Parte Especial*, p. 325; Corcoy Bidasolo / Mir Puig, *Comentarios al Código Penal. Reforma LO 5/2010*, p. 468; Tomás Valiente Lanuza, *Comentarios al Código Penal*, p. 803; Ragués i Vallès / Robles Planas, "La reforma de los delitos informáticos: incriminación de los ataques a sistemas de información", p. 372. En contra Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 485.

72 V. por todos, Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 48 y s. Una posición más restrictiva mantiene Jareño Leal, A.: *Intimidad e imagen: los límites de la protección penal*, Madrid, 2008, p. 51, para la que el bien jurídico es el secreto de las comunicaciones en tanto en cuanto suponga vulneración de la intimidad.

La acción típica consiste en interceptar las telecomunicaciones ajenas, esto es, acceder a las mismas, sin que sea preciso obstaculizarla o impedirla[73] o realizarla con tal finalidad[74,75]. La interceptación se puede realizar de cualquier forma, pero teniendo en cuenta que se trata de comunicaciones a distancia, a través de procedimientos técnicos de comunicación (cable, inalámbricos, vía satélite, etc.), la interceptación también debe realizarse mediante artificios o procedimientos también específicos y de carácter tecnológico[76]. Esta figura protege cualquier tipo de telecomunicación; la telefónica, la telegráfica, radiotelegráficas, pero también todas aquellas realizadas a través de la Red (videoconferencia, correos electrónicos, mensajería instantánea como los *chats*, *WhatsApp*, etc.)[77], sean estas orales, visuales, escritas o combinadas (voz e imagen, imagen y datos o texto, etc.), se realice con una persona física o jurídica[78], sean de carácter sincrónico o no[79].

---

73 V., entre otros, Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 95; Rueda Martín, *Protección penal de la intimidad personal e informática*, p. 46; Mata y Martín, R.: *Delincuencia informática y Derecho Penal*, Madrid, 2001, p. 130; Anarte Borrallo / Doval Pais, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", p. 450, entre otros. De otra opinión González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 308, que admite las conductas de obstaculización o desvío de las telecomunicación como un supuesto de interceptación.

74 Así, Mata y Martín, *Delincuencia informática y Derecho Penal*, p. 130.

75 Es por ello que se presenta como un delito de peligro abstracto y de mera actividad. Así, Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 99.

76 En el mismo sentido v. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 94 y s.

77 V. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 48 y s. Sin embargo, Jorge Barreiro, *Memento Práctico Penal*, n.m. 9882 considera que la interceptación de una videoconferencia debería reconducirse al tipo de utilización de artificios técnicos de grabación de cualquier señal de comunicación.

78 En el mismo sentido Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 48 y 93, citando la amplia definición de comunicación realizada por la D 2002/58/CE, de 12 de julio de 2002, sobre la privacidad de las comunicaciones.

79 Esta también parece ser la opinión de Jareño Leal, *Intimidad e imagen: los límites de la protección penal*, p. 46 y s. n. 57.

No obstante, la mayoría de los supuestos se plantearán en relación con las sincrónicas o simultáneas, pues el acceso al contenido de telecomunicaciones asíncronas (correos electrónicos, SMS, fax, etc.) quedaría cubierto por el resto de figuras delictivas del art. 197.1 CP, bien la de apoderamiento de cartas, correos electrónicos u otros documentos, bien la de utilización de artificios técnicos de grabación de cualquier señal de comunicación.

De acuerdo con lo anterior considero que el acceso a las claves bancarias de un tercero a través de un programa espía (*spyware*) podría subsumirse adecuadamente a través de esta conducta delictiva, dado que la disposición de aquellas por parte del sujeto activo tiene lugar al tiempo que se realiza la comunicación electrónica del sujeto pasivo con la entidad bancaria[80]. Y la concurrencia con el tipo de intrusismo del art. 197.3 CP, entiendo que debería resolverse mediante un concurso de leyes a favor del primero (art. 1971.1 CP), y conforme al principio de absorción o alternatividad (art. 8 CP), puesto que el bien jurídico es el mismo[81].

Sin embargo, esta figura delictiva no abarcaría las variantes de *phishing* y *pharming*, pues requiere que se intercepten las telecomunicaciones ajenas, y en ellas la comunicación tiene lugar entre la víctima y los atacantes, que se aprovechan bien del error de aquella (*phishing*), bien de la utilización de artificios técnicos (redirectores) para obstaculizar la comunicación electrónica entre la entidad bancaria y su cliente (*pharming*). Tan sólo si partiésemos de un concepto amplio de interceptación, tal y como proponen González Rus y Morales Prats, acogiendo las conductas de obstaculización (desviación) de las telecomunicaciones ajenas

80 En el mismo sentido Puente Aba, L. M.: "Delitos contra la intimidad y nuevas tecnologías", en *Eguzkilore* (21), 2007, p. 169 y s., citando jurisprudencia al respecto (en línea). Disponible en: http://www.ivac.ehu.es (último acceso: 5 de mayo de 2014).

81 También resuelve la concurrencia entre los diferentes tipos del art. 197 a través de un concurso de normas Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 143.

que tienen por finalidad la vulneración de su intimidad[82] cabría subsumir en este tipo de lo injusto la modalidad de *pharming*, que, como se acaba de señalar, consiste en la utilización de programas malignos (*malware*) para acceder al sistema informático de la víctima o al del servidor y desviar la comunicación entre la entidad bancaria y su cliente (víctima). Esta interpretación extensiva del delito, además de no ser contraria al principio de legalidad, permitiría castigar supuestos de obstaculización de las comunicaciones electrónicas que no siempre pueden reconducirse al tipo de apoderamiento de correos electrónicos o documentos del art. 197.1 CP, como se analizará más abajo.

3. Por el delito de utilización de artificios técnicos de captación de la imagen, el sonido o cualquier otra señal de comunicación

Asimismo la modalidad de *spyware* podría integrarse en la conducta del último inciso del art. 197.1 CP, que castiga la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de la imagen, el sonido o cualquier otra señal de comunicación ajenos, con la finalidad de vulnerar su intimidad[83]. En esta variante los delincuentes proceden a la grabación (reproducción o transmisión) de una señal de comunicación (electrónica) con la finalidad de atentar contra la intimidad ajena, registrando datos de carácter privado, como son las claves de acceso y de operaciones bancarias.

La conducta típica recae sobre la imagen, el sonido (voz) o cualquier señal de comunicación, entre las que incluimos las electrónicas, que también se presentan en forma de voz (sonido),

---

82 V. González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 308; de forma menos rotunda Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 455; también, aunque de forma más confusa, cft. Jareño Leal, *Intimidad e imagen: los límites de la protección penal*, p. 46 y s. y n. 57 y 47 y s.

83 Para un sector de la doctrina esta conducta formaría un único tipo de lo injusto con la interceptación de las telecomunicaciones. V. por todos Muñoz Conde, *Derecho Penal. Parte Especial*, p. 259.

imagen, y/o texto o datos[84,85]. Y el que el delito haga referencia a una señal de comunicación no implica que la conducta deba recaer sobre (tele)comunicaciones sincrónicas. En mi opinión no es preciso que la captación ilícita de la señal de comunicación se realice en el curso de una (tele)comunicación (sincrónica), porque entonces sería redundante respecto de la conducta de interceptación de las telecomunicaciones. Si esta figura delictiva prohíbe la captación clandestina de la imagen o el sonido en lugares privados (vivienda, despachos, etc.) con la finalidad de vulnerar la intimidad ajena[86], sin que sea preciso que se realice durante una comunicación, entiendo que tampoco debería exigirse en la captación clandestina (escucha, grabación, reproducción o transmisión) de cualquier otra señal de comunicación. No obstante, si bien es cierto que el precepto no establece tal requisito, tampoco lo prohíbe. Es por ello que la grabación de una conversación ajena mantenida en el domicilio o despacho de los interlocutores se podría reconducir a este delito (comunicación que no responda al concepto de comunicación a distancia por sistemas electromagnéticos)[87]. Y de la misma forma también podrían quedar cubiertos por este precepto la utilización de artificios técnicos

---

84 De forma similar v. Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 459 y s., que hace referencia a la correspondencia electrónica; Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 97.

85 No obstante, cabe plantearse si el término "señal de comunicación" se refiere al *medio de comunicación* (telefónico, telegráfico, electrónico, etc.) o, por el contrario, al *contenido de la comunicación* (imagen, sonido o voz y texto o datos). Teniendo en cuenta que esta figura delictiva se ocupa de la captación clandestina de la imagen y el sonido, considero que debemos interpretar la señal de comunicación referida al contenido de la comunicación y no al canal o medio. Haciendo referencia a esta distinción v. Lloria García, "El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de Internet. Algunas consideraciones", p. 189 y 198.

86 V. por todos Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 461; Rueda Martín, *Protección penal de la intimidad personal e informática*, p. 47 y s., que configura como un delito de peligro abstracto.

87 Así, González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 310; Jareño Leal, *Intimidad e imagen: los límites de la protección penal*, p. 52.

de captación, grabación o reproducción de una telecomunicación asíncrona (mensajes de correos electrónicos, fax, SMS, etc.) o del producto de una telecomunicación sincrónica archivada en el sistema informático (*chats* o conversaciones electrónicas), en el teléfono móvil (mensajes de *WhatsApp*) o que hayan sido grabadas (conversación telefónica, videoconferencia, etc.), algunas de las cuales podrían reconducirse asimismo al tipo de apoderamiento de documentos personales del primer inciso del art. 197.1 CP.

Cabe plantearse si este figura delictiva sería aplicable al resto de modalidades en las que la comunicación electrónica del sujeto pasivo no tiene lugar con la entidad bancaria, sino con los propios delincuentes, que se aprovechan del error de la víctima o de una manipulación informática.

En mi opinión tanto en el *phishing* como en el *pharming* el acceso a las claves bancarias por parte de los delincuentes sería, en principio, lícito, pues se realizan con el consentimiento de la víctima. Si bien en ambos supuestos concurre un error en el titular de la cuenta bancaria, provocado por el engaño o la utilización de artificios técnicos de los sujetos activos, se trataría de un error en la persona o sobre los motivos y no sobre la disponibilidad de la intimidad, por lo que serían irrelevantes[88]. En estos casos la víctima accede voluntariamente a registrar sus claves secretas en una página electrónica, y la creencia errónea de que se trata de la página de su entidad bancaria no afectaría a la validez del consentimiento[89].

---

88 Considera irrelevante el error en los motivos Luzón Peña, D. M.: *Lecciones de Derecho Penal. Parte General*, 2ª ed., Valencia, 2012, p. 379 y 281; Mir Puig, S.: *Derecho Penal. Parte General*, 9ª ed., Barcelona, 2011, p. 526. También así el Tribunal Supremo en la sentencia de 2 de octubre de 2006 (f.j. sexto) en un supuesto de abusos sexuales. De otra opinión Díez Ripollés, J. L.: *Derecho Penal Español. Parte General en esquemas*, 2ª ed., Valencia, 2009, p. 279.

89 En el mismo sentido v. Goeckenjan, "Auswierkungen des 41. des Strafrechtsänderungsgesetzes auf die Strafbarkeit des Phishing", p. 50. Popp, "Von Datendieben und Betrügern zur Strafbarkeit des sogennanten Phishing", p. 3518.

Pero no es menos cierto que en ambas modalidades se produciría además del acceso a datos personales ajenos, contando con el consentimiento de su titular, su grabación en el curso de una (tele)comunicación electrónica[90]. Esta grabación, como ya se ha visto, no podría reconducirse al tipo de la interceptación de las comunicaciones, porque se trataría de una grabación sobre una comunicación propia, aun cuando se realizase sin la autorización del otro cotitular de la comunicación. Y por la misma razón la doctrina mayoritaria también rechaza la consideración de esta figura de utilización de artificios técnicos de grabación (escucha, retransmisión o reproducción) de cualquier señal de comunicación (voz, imagen o datos)[91,92].

No obstante, un sector de la doctrina, cada vez más numeroso (Jareño Leal, Juanatey Dorado, Doval Pais, Valeije Álvarez y Tomás Valiente Lanuza, entre otros), al que me sumo, defiende la ilicitud de tales conductas, al considerar que el consentimiento en la cesión o revelación de información personal privada al otro interlocutor no alcanzaría a la grabación clandestina, entre otras razones, por representar un plus de intromisión ilegítima en la intimidad[93,94]. De esta forma la utilización de

90 Salvo que los delincuentes memorizaran o anotaran la información sin necesidad de la utilización de artificios técnicos de grabación, reproducción o transmisión.

91 V. por todos Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 98, citando doctrina y jurisprudencia. En contra Muñoz Conde, *Derecho Penal. Parte Especial*, p. 259 y Juanatey Dorado, C. / Doval Pais, A.: "Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes", en *La protección jurídica de la intimidad*: J. Boix Reig, Madrid, 2010, p. 141 y s., 152 y ss., 166 y ss.

92 En cambio, sí sería típica tal conducta si la realizase un tercero, distinto de los interlocutores de la comunicación, que no contase con el consentimiento de aquellos. V. por todos Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 98.

93 Así, como hemos visto, Juanatey Dorado / Doval Pais, "Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes", p. 141 y s., 152 y ss., 166 y ss., con múltiples argumentos y referencias judiciales. Y ya antes v. Jareño Leal, *Intimidad e imagen: los límites de la protección penal*, p. 97 y ss.; Valeije Álvarez, I.: "Intimidad y

artificios técnicos de grabación o transmisión de la imagen, el sonido o cualquier otra señal de comunicación que puedan afectar a la intimidad personal, realizados sin el consentimiento de su titular, serían típicos. Tales supuestos si bien no vulnerarían, en su caso, el secreto de las comunicaciones, protegido en la conducta de interceptación de las telecomunicaciones, sí lo harían con la intimidad, bien jurídico protegido en el delito de utilización de artificios técnicos de grabación analizado[95].

De acuerdo con esta posición doctrinal y jurisprudencial cabría castigar por este última figura delictiva tanto la variante de *pharming* como la de *phishing*, pues en ambas el sujeto activo procede a la grabación (reproducción o transmisión) de una señal de comunicación (electrónica) con la finalidad de atentar contra la

---

difusión de imágenes", en *Constitución, derechos fundamentales y sistema penal*: J. C. Carbonell Mateu / J. L. González Cussac / E. Orts Berenguer (Dir.), Valencia, 2009, p. 1868 y ss.; Tomás Valiente Lanuza, *Comentarios al Código Penal*, p. 797. En sentido semejante cft. Serrano Gómez, A. / Serrano Maíllo, A.: *Derecho Penal. Parte Especial*, 16ª ed., Madrid, 2011, p. 280. También v. en este sentido la STS de 10 de diciembre de 2004 (f.j. octavo), por el que se condena a una mujer por la grabación de una relación sexual mantenida con otro sujeto, sin su consentimiento. En la misma línea que estos autores, el Tribunal Supremo considera que tales conductas atentan gravemente contra la intimidad ajena por la "especial insiosidad del medio empleado" (artificio técnico de grabación), no admitiendo la doctrina de la "intimidad compartida" para excluir la tipicidad de la misma.

94 Si bien estos autores se refieren a supuestos de grabación de la imagen o el sonido, considero que a la misma conclusión debería llegarse con cualquier otra señal de comunicación.

95 En el mismo sentido v. la STS de 10 de diciembre de 2010 (f.j. octavo), que, siguiendo la jurisprudencia del Tribunal Constitucional, lo extiende no solo a los casos de grabaciones de contenido sexual por parte de uno de los protagonistas de la relación, sin el consentimiento del otro, sino también a aquellos en los que el interlocutor de una conversación telefónica de contenido íntimo la graba sin el consentimiento del afectado. Y de la misma forma los casos de revelación del contenido íntimo de una carta por parte del destinatario, sin la autorización del remitente y titular de la intimidad contenida en aquella; o en aquellos otros en los que un interlocutor de una conversación telefónica, pulsa el altavoz del teléfono, sin el consentimiento del otro, descubriendo sus secretos a terceros.

intimidad ajena, registrando datos privados, como son las claves de acceso y de operaciones bancarias[96].

A la misma solución se llegaría si se partiese de la posición doctrinal que considera que un error en los motivos vicia el consentimiento prestado, convirtiendo en ilícito el acceso a las claves bancarias. Y siendo el acceso ilícito, también lo sería la grabación o registro de los datos.

El posible concurso entre los tipos de interceptación de las comunicaciones y utilización de artificios técnicos de grabación de cualquier señal de comunicación en las modalidades de *spyware* y *pharming* debería resolverse a través de las reglas del concurso de leyes[97]. Para el *spyware* considero más adecuada el tipo de interceptación de las comunicaciones. Más compleja resulta la solución del *pharming*, pues ambas propuestas parten de posiciones doctrinales minoritarias.

En cambio, la vulneración de la intimidad en la modalidad del *phishing*, tan sólo podría reconducirse al tipo de utilización de artificios técnicos de grabación de una señal de comunicación, siempre que aceptemos, o bien que el error en los motivos excluye el consentimiento, posición que no me convence, o bien que la grabación de los datos bancarios sin el consentimiento de su titular es ilícita, aun cuando haya sido realizada por el otro interlocutor de la comunicación.

---

96 El Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, de 1 de octubre de 2013 (BOCCGG de 4 de octubre de 2013) tampoco resuelve esta cuestión. La nueva figura delictiva prevista en el art. 197.4 bis CP castiga la difusión, revelación o cesión a terceros de imágenes o grabaciones audiovisuales de otro, sin su consentimiento, pero no así la grabación de tales imágenes. Por otro lado, injustificadamente, el objeto material se centra en imágenes y grabaciones audiovisuales, dejando fuera las grabaciones, reproducciones o copias de audio y texto o datos.

97 También así Anarte Borrallo / Doval Pais, *Derecho Penal. Parte Especial. Vol. I*, p. 451; Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 143. En cambio defiende un concurso (real) de delitos Rueda Martín, *Protección penal de la intimidad personal e informática*, p. 65.

4. Por el delito contra los datos reservados de carácter personal o familiar

En contra de la posición mantenida hasta ahora por la doctrina, no considero de aplicación a estas conductas el delito del art. 197.2 CP[98].

Este precepto castiga el acceso, apoderamiento, modificación o utilización de datos reservados de carácter personal o familiar registrados en archivos y registros (electrónicos) públicos o privados, garantizando así el derecho fundamental a la protección de los datos personales del art. 18.4 CE[99]. Sin embargo, ninguna de las variantes de *phishing* (en sentido amplio) analizadas responde a esta figura delictiva, pues aunque en ellas el sujeto accede o se apodera de datos personales ajenos de carácter reservado (las claves bancarias), sin estar autorizado y en perjuicio de terceros, estos no se encuentran registrados en ficheros, soportes, archivos o registros, tal y como exige esta conducta delictiva, esto es, no se encuentran registrados en bases de datos organizadas.

El objeto material de este precepto son, por tanto, los datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Tanto la interpretación objetiva como la sistemática del precepto[100] y el propio bien jurídico (el derecho a la autodeterminación informativa o derecho al control de los datos personales)

---

98 Defienden en estos casos la apreciación del art. 197.2 CP Rey Ruidobro, L. F.: "La estafa informática: relevancia penal del *phishing* y el *pharming*", en *Diario La Ley* (7926), 2012, p. 9 y s. (en línea). Disponible en: http://www.laleydigital.es (último acceso: 6 de agosto de 2013); Velasco Núñez, "Delitos informáticos realizados en actuación organizada", p. 12; el mismo "Estafa informática y banda organizada", p. 23; el mismo "Fraudes informáticos en la red: del *phishing* al *pharming*", p. 61.

99 V. por todos Romeo Casabona, Los delitos de descubrimiento y revelación de secretos, p. 40 y ss.

100 A esta conclusión se llega si ponemos en relación el tipo del 197.2 CP con el tipo del 197.4 CP, que recoge un tipo agravado para los casos en los que el sujeto activo sea la persona encargada del fichero electrónico.

Estudios Penales y Criminológicos, vol. XXXIV (2014). ISSN 1137-7550: 301-339

nos conducen a considerar que los términos "fichero" y "soporte" informáticos se corresponden con los de archivo o registro, esto es, almacenamiento organizado de datos[101]. Por tanto, el acceso o apoderamiento de datos personales ajenos de carácter reservado que se hallen recogidos en ficheros electrónicos o soportes informáticos (disco duro, memoria externa, CD, etc.) que no formen parte de un archivo, registro o fichero organizado quedarían fuera de este delito[102].

5. Por el delito de apoderamiento de documentos o efectos personales

Tampoco resulta adecuada para sancionar el *phishing* (en sentido amplio) la figura de apoderamiento de documentos y efectos personales para descubrir los secretos o vulnerar la intimidad de otro, prevista en el art. 197.1 CP. En primer lugar por las dudas que plantea la acción típica de apoderamiento. Así, mientras un grupo de autores exige el desplazamiento físico del objeto material o al menos la pérdida de control por parte del sujeto pasivo, siguiendo el concepto de apoderamiento o sustracción de los delitos patrimoniales[103], otro sector doctrinal mantiene un

---

101 Sobre esta cuestión y sobre las dudas que plantea el término "soporte" v. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 113 y s. También considerando que los datos reservados de carácter personal o familiar deben estar registrados en ficheros o archivos Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 467 y 473; Mata y Martín, "El robo de identidad: ¿una figura necesaria?", p. 213; Puente Aba, "Delitos contra la intimidad y nuevas tecnologías", p. 166 y 168; Gómez Navajas, *La protección de los datos personales*, p. 133 y 147; Rueda Martín, *Protección penal de la intimidad personal*, p. 76. También en este sentido v. la STS de 30 de diciembre de 2009 (f.j. sexto).

102 De otra opinión Bacigalupo Zapater, E.: "Documentos electrónicos y delitos de falsedad documental", en *Delincuencia informática. Problemas de responsabilidad*: O. Morales García (Dir.), Cuadernos de Derecho Judicial, Madrid, 2002, p. 295. También de forma aislada v. la SAP de Huesca, de 18 de julio de 2013 (f.j. 2).

103 Así, Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 457. Por ello interpreta que el apoderamiento de los correos electrónicos

concepto amplio del término, adaptado al bien jurídico protegido. En este sentido se considera que una interpretación teleológica del precepto admitiría tanto la sustracción de los efectos personales del sujeto pasivo, como la realización de una fotocopia o fotografía de los documentos y efectos personales, grabación del correo electrónico[104,105], así como la simple captación del secreto, siempre que haya un comportamiento que facilite el acceso al objeto material (vulneración de contraseñas, utilización de programas rastreadores o *sniffers*)[106]. Tal interpretación no requiere que el sujeto pasivo quede desposeído del objeto material.

En segundo lugar porque el precepto exige que el sujeto se apodere no de los secretos o información personal privada, sino de los correos electrónicos, documentos o efectos personales que sean idóneos para contenerlos, debiendo existir además identidad entre

---

debe entenderse como sustracción de una copia impresa del mismo o, en todo caso, como captación intelectual sin desplazamiento físico, pues cualquier otra captación del correo podría reconducirse al resto de tipos de lo injusto del art. 197.1 CP. V. ob. cit., p. 455. En el mismo sentido Anarte Borrallo / Doval Pais, *Derecho Penal. Parte Especial. Vol. I*, p. 449.

104 Así también González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 306; Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 83 y ss.; Rueda Martín, *Protección penal de la intimidad personal*, p. 42 y s. De forma similar Mata y Martín, *Delincuencia informática y Derecho Penal*, p. 128 y s., para el que el apoderamiento no exige la desposesión del efecto o documento ajeno para su titular, sino la apropiación del contenido del documento mediante algún tipo de materialización (impresión o copia del documento electrónico). Esta también es la posición mantenida por la jurisprudencia, de la que informa Jareño Leal, *Intimidad e imagen: los límites de la protección penal*, p. 36 y ss. (39).

105 Objeto de mayor discusión plantea la interceptación o desvío del correo electrónico. Defendiendo su subsunción en este tipo de lo injusto v. Romeo Casabona, *Los delitos de descubrimiento y revelación de secretos*, p. 89 y s. Manteniendo que constituiría un supuesto de interceptación de las telecomunicaciones Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 455; González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 306.

106 Así González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 305; Romeo Casabona *Los delitos de descubrimiento y revelación de secretos*, p. 93; Orts Berenguer / Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática*, p. 26 y s.

el sujeto pasivo y el titular del objeto material[107]. Sin embargo, en las conductas de *phishing* (en sentido amplio) el sujeto accede a las claves y contraseñas bancarias, electrónicamente, a través de la Red; accede o se "apodera" directamente de estos datos personales de carácter privado, secreto o, en todo caso, reservado, sin necesidad de apropiarse de documentos o efectos personales que los pudiesen contener, tal y como exige el precepto[108]. Por tanto, estas conductas solo se podrán subsumir en este delito si consideramos que tales datos personales constituyen el objeto material de la conducta, esto es, un documento o efecto personal del sujeto pasivo. El efecto personal debe descartarse, pues ha sido definido como todo objeto material personal que posea un contenido de intimidad para el sujeto pasivo[109]. La respuesta entonces sólo puede estar en el documento, definido a estos efectos en el art. 26 CP. Si bien este precepto también hace mención a la necesidad de un "soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica", doctrina y jurisprudencia mantienen que los documentos electrónicos quedarían cubiertos por este concepto. En estos el soporte material estaría constituido por el ordenador, disco duro externo, disquete, memoria electrónica, tarjeta electromagnética, microfilm, soportes ópticos, etc. que lo

107 Así, Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 457.

108 Sin perjuicio de que si así fuese, al utilizarse, por ejemplo, un programa informático (*malware*) que permitiese acceder a las claves bancarias recogidas en un correo electrónico o cualquier otro documento electrónico alojado en la memoria del sistema informático, no hubiese inconveniente en apreciar este tipo delito. Un caso similar recoge la sentencia del Juzgado de lo Penal de Badajoz, de 15 de febrero de 2006, que condena por esta figura (y no por la del art. 278.1 CP, más apropiada para el supuesto de hecho del que se ocupaba) a un intruso que accede a través de la Red al sistema informático de una empresa y se apodera de los códigos de acceso de un juego informático (permiso de administrador), así como de los correos electrónicos de los empleados y datos de cuentas de usuarios.

109 Así, Romeo Casabona *Los delitos de descubrimiento y revelación de secretos*, p. 81; Morales Prats, *Comentarios a la Parte Especial del Derecho Penal*, p. 455.

albergase[110,111], sin que constituya un obstáculo el que su contenido haya de ser determinado indirectamente mediante la utilización de un aparato lector[112]. Más dudas plantea la adecuación de los documentos encriptados (firma electrónica, claves electrónicas bancarias, etc.) al concepto del art. 26 CP[113]. Pero difícilmente los documentos electrónicos cumplen con la garantía de perpetuidad exigida tradicionalmente si la información tan sólo se halla alojada en la memoria RAM del sistema, constituyendo un

---

110 En este sentido v. Muñoz Conde, *Derecho Penal. Parte Especial*, p. 677; Mir Puig, C.: "Sobre algunas cuestiones relevantes del Derecho Penal en Internet", en *Internet y Derecho Penal*: J. J. López Ortega (Dir.), Cuadernos de Derecho Judicial (X), Madrid, 2001, p. 287 y ss., para el que el citado precepto recoge un concepto material de documento; García Cantizano, M. C.: *Falsedades documentales en el Código Penal de 1995*, Tirant lo Blanch, Valencia, 1997, p. 62 y ss.; De Urbano Castrillo, E.: "El documento electrónico: aspectos procesales", en *Internet y Derecho Penal*: J. J. López Ortega (Dir.), Cuadernos de Derecho Judicial (X), Madrid, 2001, p. 558 y ss. También de forma favorable se han pronunciado González Rus, *Sistema de Derecho Penal Español. Parte Especial*, p. 306; Fraile Coloma, C.: *Comentarios al Código Penal*: M. Gómez Tomillo (Dir.), 2ª ed., Valladolid, 2011, p. 235 y s.

111 V. STS de 22 de abril de 1998 (f.j. quinto) y siguiendo a la anterior y a otras muchas resoluciones en este sentido v. STS de 13 de septiembre de 2002 (f.j. primero).

112 De Urbano Castrillo, "El documento electrónico: aspectos procesales", p. 561 y 571; García Cantizano, *Falsedades documentales en el Código Penal de 1995*, p. 66 y ss.

113 A favor de su inclusión v. Morales García, O.: "Malversación, estafa y falsedad en documento electrónico. Algunas reflexiones sobre la STS de 30 de octubre de 1998", en *El nuevo Derecho Penal Español. Estudios penales en memoria del profesor José Valle Muñiz*: G. Quintero Olivares y F. Morales Prats (Coords.), Pamplona, 2001, p. 1596 y ss., al responder a las garantías de confidencialidad, integridad y perpetuación de los datos, así como a la de identidad del autor; C. Mir Puig, "Sobre algunas cuestiones relevantes del Derecho Penal en Internet", p. 290 y ss. (297), para el que la firma digital o electrónica constituye un documento electrónico, aunque se halle encriptado, al poder ser atribuible a una persona y cumplir con la garantía de integridad. En el mismo sentido v. De Urbano Castrillo, "El documento electrónico: aspectos procesales", p. 561. En contra de que los documentos encriptados respondan al concepto del art. 26 CP, v. Cugat Mauri, M.: "Sistema Penal (I) Código Penal 1995", en *Actualidad Penal* (1-116), 2000, y las resoluciones del Tribunal Supremo más arriba señaladas.

mero documento virtual[114], tal y como ocurre generalmente en todas las modalidades de *phishing* (en sentido amplio). Por ello para cumplir con las exigencias de integridad de la declaración de voluntad se exige que los documentos electrónicos queden contenidos en un soporte material de cualquier tipo (disquete, memoria electrónica, tarjeta magnética, etc.) o en el disco duro del sistema informático, no siendo suficiente la memoria RAM[115].

III. Consideraciones finales sobre la respuesta penal a la obtención subrepticia de datos personales relativos a la identidad en el *phishing* bancario

De acuerdo con lo expuesto en la segunda parte de este trabajo, se puede afirmar que los actuales tipos de lo injusto del Título X, Capítulo Primero de nuestro Código Penal abarcarían la primera fase del *phishing* bancario en sus diversas variantes[116]. Esta fase, como se ha analizado en la primera parte de este estudio, se corresponde a su vez con el mal denominado "robo de identidad", propia de otro complejo fenómeno criminal conocido por *identity related crime*.

Cuando el *phishing* (en sentido amplio) recaiga sobre claves y contraseñas bancarias correspondientes a una persona jurídica y, en cualquier caso, cuando nos enfrentamos con la variante de *pharming* dirigido al servidor DNS el tipo de lo injusto a tener en cuenta será el del art. 200 CP, que castiga el descubri-

---

114 Como así ha sido denominado por Rovira del Canto, E.: "Tratamiento penal sustantivo de la falsificación informática", en *Internet y Derecho Penal*: J.J. López Ortega (Dir.), Cuadernos de Derecho Judicial (X), Madrid, 2001, p. 480, diferenciándolo de los documentos electrónicos.

115 Así lo han defendido Rovira del Canto, "Tratamiento penal sustantivo de la falsificación informática", p. 480; De Urbano Castrillo, "El documento electrónico: aspectos procesales", p. 558; Davara Rodríguez, M. A.: *Manual de Derecho Informático*, 10ª ed., Cizur Menor, 2008, p. 439.

116 A diferencia de lo que ocurre con otros códigos penales, por ejemplo, el alemán. En este sentido v. la crítica de Goeckenjan, "Auswierkungen des 41. des Strafrechtsänderungsgesetzes auf die Strafbarkeit des Phishing", p. 54.

miento clandestino de datos reservados de una persona jurídica. En cambio, si las conductas de acceso u obtención ilícita tienen como objeto las claves bancarias de una persona física, tanto la modalidad a través de programas espía o *spyware* como la de uso de redirectores o *pharming* (local y a través de *router*) integrarían la figura de intrusismo informático del art. 197.3 CP. Asimismo el acceso no consentido a las claves bancarias del *spyware* supondría una interceptación de las comunicaciones del art. 197.1 CP, e incluso el *pharming*, si partiésemos de una interpretación extensiva de la acción típica. Por otro lado, el *pharming* podría quedar cubierto también, junto con el *phishing* (ahora en sentido restringido), por la conducta típica de grabación de una señal de comunicación del art. 197.1 CP, a salvo de ciertas cautelas o condiciones. En primer lugar, que admitiésemos como señal de comunicación la grabación de datos y no sólo la de la imagen o el sonido. En segundo lugar, que consideráramos que en este delito la grabación, reproducción o transmisión de los datos sin consentimiento de su titular es típica aun cuando se realizase por uno de los interlocutores de la comunicación, pues el consentimiento en la cesión o revelación de información personal privada al otro interlocutor no supondría una autorización para su grabación.

En la mayoría de los supuestos podrían apreciarse asimismo las agravaciones previstas en los números 7 y 8 del art. 197 CP, dado que las conductas de *phishing* (en sentido amplio) persiguen fines lucrativos y se realizan en el seno de una organización criminal[117].

La concurrencia de los diferentes tipos de lo injusto daría lugar a un concurso de leyes, a resolver por el principio de consunción del art. 8.3 CP a favor de las conductas del art. 197.1 CP[118]. A su vez, la responsabilidad penal por estas conductas

117 Y ello, sin perjuicio de la responsabilidad penal por su participación en una organización criminal del art. 570 bis CP, pues partimos de bienes jurídicos diferentes. De otra opinión v. Velasco Núñez, "Delitos informáticos realizados en actuación organizada", p. 11.

118 En cambio, los supuestos de *phishing* ejecutados con anterioridad a la entrada en vigor del art. 197.3 CP (23 de diciembre de 2010) tan sólo responderían

entraría en concurso real de delitos con los tipos delictivos de las sucesivas fases: con la estafa informática del art. 248.2 a) CP de la segunda, y con la participación en el blanqueo de capitales ejecutado por los intermediarios (muleros) de la tercera (art. 301 CP), además de con la figura prevista en el art. 570 bis CP por la participación en organización criminal.

De no admitirse la interpretación propuesta del tipo de lo injusto de grabación de una señal de comunicación o incluso la más discutible de la relevancia del error sobre los motivos, la modalidad de pesca de datos (*phishing*) no supondría un atentado a la intimidad, mientras que la variante de redirectores (*pharming*) tan sólo podría castigarse por intrusismo informático[119], salvo que se admita que la obstaculización de la telecomunicación también forma parte de la conducta típica de interceptación de las comunicaciones.

Por ello, aunque no estrictamente necesaria, sí sería conveniente una revisión del Código Penal a fin de adaptarlo a estas y otras nuevas formas de criminalidad[120].

En el ámbito de las conductas analizadas la posible revisión del Código Penal debería ir orientada a señalar que la transmisión, grabación o reproducción clandestina de la imagen, el sonido o cualquier otra señal de comunicación abarca, sin ningún género de dudas, la comunicación realizada a través de texto o datos, con independencia de que fuese ejecutada por un tercero o por uno de los titulares de la propia comunicación. Pero la adaptación de nuestro texto penal a este fenómeno criminal también podría resolverse si el acceso u obtención no consentida de los datos

---

por el delito de interceptación de las comunicaciones o, en su caso, por el de grabación de una señal de comunicación.

119 Y ello siempre que se hubiese cometido tras la entrada en vigor de este precepto (23 de diciembre de 2010), pues de haberse ejecutado con anterioridad también quedaría impune.

120 En el mismo sentido en relación con la necesidad de revisar los delitos de falsedades documentales a fin de que los documentos y la firma electrónicos puedan ser protegidos plenamente v. Bacigalupo Zapater, "Documentos electrónicos y delitos de falsedad documental", p. 304.

personales cubiertos por la intimidad o por la libertad informática pudiese tener acogida en el delito de acceso no consentido a datos reservados de carácter personal o familiar del art. 197.2 CP o, en último extremo, en el de apoderamiento de documentos o efectos personales ajenos del art. 197.1 CP. En el primer caso admitiendo que la conducta típica pueda recaer sobre datos reservados de carácter personal (o familiar), aun cuando no formen parte de un archivo o registro (base de datos organizada)[121]. En el segundo, ampliando el objeto material del delito a los datos personales de carácter electrónico directamente y no solo a los contenidos en documentos o efectos personales.

121 Defienden este alcance de *lege lata* Rey Ruidobro, "La estafa informática: relevancia penal del *phishing* y el *pharming*", p. 9 y s.; Velasco Núñez, "Delitos informáticos realizados en actuación organizada", p. 12.