IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Dosier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»

ARTÍCULO

El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento

Beatriz López Pesquera
Agencia provincial de Barcelona
UOC

Fecha de presentación: mayo de 2018
Fecha de aceptación: julio de 2018
Fecha de publicación: septiembre de 2018

Resumen

Con ocasión de las ventajas que ofrecen las tecnologías de la sociedad de la información y las redes sociales han proliferado conductas ilícitas centradas, principalmente, en delitos patrimoniales. Las conductas más habituales son aquellas destinadas a la compraventa de productos de segunda mano, las que exponen un modo de vida constituyéndose en *influencers*, o los delitos relativos a la publicidad engañosa, entre otros, aunque el abanico delictual es mucho más amplio. El estudio desvela que, en cualquier caso, no se trata de estafas informáticas propiamente dichas; el número de perjudicados es muy numeroso, existiendo, además, importantes dificultades en su investigación, por no mencionar la concurrencia de problemas concursales en no pocos casos.

Palabras clave

redes sociales, estafa, delito informático, delitos patrimoniales

Tema

Derecho penal

Fraud committed via social networks: research and indictment problems

Abstract

There has been a rise of illegal acts based on the advantages offered by ICT and social networks, mainly based on crimes against property. The most common acts are those relating to the purchase or sale of second-hand products, those exhibiting an influencer lifestyle or crimes relating to misleading advertising, among others. However, the complete range of crimes is much broader. The study reveals that, in any case, these are not ICT scams per se, as the number of parties suffering damages is very high. Its research also poses significant difficulties, as in many cases it does not mention the occurrence of bankruptcy problems.

Keywords

social networks, fraud, computer crime, crimes against property

Topic

Criminal Law

1. Aproximación a los conceptos

En el presente trabajo trataremos de analizar los principales problemas que la investigación y el enjuiciamiento de los delitos de estafa cometidos a través de las redes sociales plantean. Sin embargo, con carácter previo convendría definir algunos conceptos.

El **delito de estafa** aparece recogido en el artículo 248.1 del Código penal, según el cual «cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno».

El Tribunal Supremo ha enumerado los elementos exigidos en el tipo penal en el artículo 248.1 del Código penal en numerosas ocasiones:[1]

1. Un engaño precedente o concurrente.
2. Dicho engaño ha de ser bastante para la consecución de los fines propuestos, con suficiente entidad para provocar el traspaso patrimonial.
3. Producción de un error esencial en el sujeto pasivo, desconocedor de la situación real.
4. Un acto de disposición patrimonial por parte del sujeto pasivo, con el consiguiente perjuicio para el mismo.
5. Nexo causal entre el engaño del autor y el perjuicio a la víctima.
6. Ánimo de lucro.

El elemento característico del delito de estafa, como es bien sabido, es el «engaño bastante». La jurisprudencia del Tribunal Supremo ha venido configurando el engaño típico en no pocas sentencias[2] como «aquel que genera un riesgo jurídicamente desaprobado para el bien jurídico tutelado y concretamente el idóneo o adecuado para provocar el error determinante de la injusta disminución del patrimonio ajeno».

En torno al engaño bastante se han suscitado muchas cuestiones que exceden del objeto de este trabajo; sin embargo, me gustaría poder traer a colación alguna de ellas por la relevancia que pueda tener en los supuestos que se analizarán.

1. *Vid*. STS 810/2016, de 28 de octubre, con cita, entre otras a la STS 880/2005, de 4 de julio.
2. *Vid*. SSTS 564/2007, 162/2012, de 23 de diciembre.

Se ha planteado la autotutela como causa de exclusión de la tipicidad en estos delitos, si bien el Tribunal Supremo ha establecido[3] que una cosa es la exclusión del delito de estafa en supuestos de «engaño burdo» o de «absoluta falta de perspicacia, estúpida credulidad o extraordinaria indolencia», y otra que se pretenda desplazar sobre la víctima de estos delitos la responsabilidad del engaño, exigiendo un modelo de autoprotección o autotutela que no está definido en el tipo penal ni se reclama en otras infracciones patrimoniales. No resulta procedente, por ello, renunciar a la intervención penal a favor de la autotutela de la víctima, desconociendo que constituye un principio básico del ordenamiento jurídico el de que los ciudadanos han hecho dejación de la respuesta punitiva en manos del Poder Judicial precisamente para descargarse de sus necesidades defensivas frente a las agresiones legalmente tipificadas como delictivas.

La configuración del concepto «engaño bastante para producir error en otro» implica la necesaria relación entre un sujeto activo y un sujeto pasivo. Antes del Código penal de 1995, dicha configuración planteaba problemas tanto para la doctrina como para la jurisprudencia al tratar de calificar jurídicamente determinados hechos, fundamentalmente las transferencias no consentidas de dinero ajeno, puesto que se partía de la premisa de que no se podía engañar a una máquina.

Como decíamos, el Código penal de 1995, ya en su redacción original, vino a resolver la cuestión en el apartado 2.º del artículo 248 CP tipificando las denominadas estafas impropias de la siguiente manera: «También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero»; por su parte, el apartado 3.º del artículo 248 CP establecía que se aplicaría la misma pena «a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador especialmente destinados a la comisión de las estafas previstas en este artículo» (conductas, estas últimas, en las que no se habría producido perjuicio patrimonial alguno, todavía).

El vigente artículo 248.2 del Código penal engloba los originales apartados 2.º y 3.º y añade una conducta más, sancionada con idéntica pena para «los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero».

Por lo que respecta al concepto de **delitos informáticos**, el Convenio sobre Cibercriminalidad (Budapest, 23 noviembre de 2001), en el seno del Consejo de Europa,[4] en su preámbulo indica la necesidad de establecer mecanismos de prevención, incriminación de las conductas en él descritas y atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales.[5]

Podemos conceptuar los delitos informáticos[6] como «aquellas conductas típicas, antijurídicas, culpables y debidamente sancionadas por el ordenamiento jurídico penal para cuya ejecución se valen de ordenadores, computadoras o cualquier otro mecanismo electrónico o informático, bien como medio, bien como fin, o mediante el uso indebido de los mismos».

El Convenio de Budapest nos ofrece un concepto de **estafas informáticas** en su artículo 8, indicando que «los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;

3. *Vid*. SSTS 162/2012, de 15 de marzo; 243/2012, de 30 de marzo; y 344/2013, de 30 de abril.
4. Instrumento de ratificación publicado en el BOE de 17 de septiembre de 2010.
5. En el preámbulo del Convenio de Budapest se indica la necesidad del mismo: «Para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable».
6. Así los conceptúa Rey Huidobro (2013).

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona».

Dentro del concepto «estafas informáticas» propiamente dichas podemos incluir el *phising*, el *smishing* y el *pharming*, cuyo estudio excede del objeto de este trabajo.[7]

La RAE define **red social** como la plataforma digital de comunicación global que pone en contacto a un gran número de usuarios. Si acudimos al Observatorio Tecnológico del Ministerio de Educación, Cultura y Deporte, encontramos una definición más extensa: se trata de «estructuras sociales compuestas por un grupo de personas que comparten un interés común, relación o actividad a través de internet, donde tienen lugar los encuentros sociales y se muestran las preferencias de consumo de información mediante la comunicación, en tiempo real, aunque también puede darse la comunicación diferida en el tiempo, como en el caso de los foros».[8]

2. Las estafas y las redes sociales. Problemas prácticos en su investigación

Resulta una obviedad señalar que, en los últimos años, hemos asistido a la proliferación de las redes sociales en general y a la de aquellas destinadas a la compraventa de productos de segunda mano, en particular. Es en el ámbito de estas últimas donde fijaremos nuestra atención para analizar los problemas que se suscitan ante la comisión de delitos de estafa.

En la estafa «tipo» de la que se parte, la básica, una persona, el vendedor, oferta un producto determinado en una red social, entra en contacto con el comprador, quien deberá efectuar el ingreso de la cantidad concertada con carácter previo a la recepción del producto, si bien dicho producto nunca llegará a su destinatario, quien tras varios intentos, todos ellos infructuosos, por resolver el problema, finalmente, en el mejor de los casos, optará por interponer la denuncia correspondiente. En otras modalidades, el comprador efectúa el ingreso acordado, o bien, lo hace a cargo de la cuenta de un tercero desconocedor de la operación, o lo hace a cargo de una cuenta bancaria de su titularidad (real o ficticia, con lo que podríamos encontrarnos ante otros ilícitos penales); efectuado el ingreso y remitido el comprobante al vendedor, una vez obtiene el producto en cuestión, anula el cargo o este es anulado por el titular de la cuenta bancaria ajeno a la defraudación cuando se percata del cargo.

La primera cuestión que podemos plantearnos es si estamos ante auténticas estafas informáticas; la respuesta, en términos generales, debe ser negativa, como ya se apuntaba en la Instrucción FGE 2/2011.[9] Se trata de estafas comunes, sin perjuicio de que se haya utilizado la tecnología

7. Véase Velasco Núñez (2008).
El *phising*, generalmente, se realiza enviando mensajes de correo electrónico reportados desde diversos sitios de la red (pero también a través de virus o enlaces de páginas web), principalmente a usuarios de la banca informática en cuyos textos, haciéndose pasar por los servicios de seguridad del banco, apremian y urgen a los usuarios –a veces bajo amenazas de anular la cuenta– a conectarse a una página web perfectamente imitada, pero falsa, y en ella a ceder los códigos de acceso y contraseñas secretas de seguridad, que una vez conocidas por los delincuentes, les permiten usarlas y quedarse con el dinero de sus víctimas. [...] En el *smishing* (*phising* por SMS) se suelen enviar los mensajes a través del teléfono móvil y lo que se pide en sus textos engañosos son el número de tarjeta y la fecha de caducidad, con esa información se confeccionan tarjetas de crédito falsas (*skimming*) para adquirir productos en el mercado, cargados contra la cuenta asociada del engañado. [...] El *pharming* consiste en una modificación técnica de las direcciones DNS (*domain name server*) del servidor informático o del archivo *host* del PC, hecha por el *pharmer*, tras la que, quien teclea en la barra del buscador las señas (generalmente de bancos en línea) no accede a la página web solicitada, sino a otra perfectamente imitada a la que el servidor le redirecciona y en la que se ponen sin querer y sin saber los datos y claves secretas del usuario bancario, por creer estar usando sus servicios al creer estar en la web del banco, claves que luego son usadas por el delincuente para realizar a su favor transferencias no consentidas por el titular, a quien le indican que en ese momento no pueden atender por razones técnicas.
8. Véase Ponce Idatzia (2012).
9. La Instrucción 2/2011, de la Fiscalía General del Estado, sobre el Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías, tras exponer la necesidad de la especialización en esta materia, configura el marco competencial de la misma y señala que «efectivamente, junto a tipos penales a través de los cuales el legislador ha protegido específicamente la seguridad de los datos, programas y/o sistemas informáticos, existen otras conductas ilícitas que, afectando a los más diversos bienes jurídicos, se planifican

para su comisión (básicamente, para que el sujeto activo y el pasivo entren en contacto), pero sin que haya existido una manipulación informática o un artificio semejante, como exige el apartado 2.º del artículo 248 CP.

El encontrarnos ante estafas comunes no implica que no se susciten problemas prácticos. Hace años, un ladrón atracaba un banco y robaba un millón de euros; ahora, ese mismo ladrón, sin necesidad de salir de su casa, puede robar un euro a un millón de personas. Esta nueva realidad conlleva una problemática propia en la investigación de tales hechos. En primer lugar, no se puede ignorar el riesgo de impunidad de muchas de estas conductas precisamente por la escasa cuantía de alguno de estos fraudes que determina que las víctimas opten por no denunciar el delito, que ponderen el perjuicio económico sufrido con las molestias/inconvenientes que les puede suponer interponer una denuncia e iniciar, así, un procedimiento penal.

A ello debemos añadir que el número de potenciales víctimas de estas estafas puede ser elevado, puesto que serán tantas como pudieran tener acceso a la información difundida y la dispersión geográfica de las mismas, lo que puede acentuar el riesgo de impunidad del que hablábamos anteriormente.

Superado el momento de interponer la denuncia por la víctima, aparecen nuevas cuestiones.

El Acuerdo del Pleno no jurisdiccional del Tribunal Supremo del 3 de febrero de 2005 resolvió la cuestión de la competencia para la instrucción de los delitos de estafa al consagrar la regla de la ubicuidad, según la cual «el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo; en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa».

Uno de los principales problemas a la hora de investigar una estafa de este tipo radica en la dificultad para identificar y localizar al presunto autor de la misma. Partiendo de la estafa «tipo» que hemos descrito en párrafos anteriores, si el sujeto facilitó un número de cuenta donde efectuar el ingreso de su titularidad, la identificación resultará sencilla, puesto que la entidad bancaria en cuestión indicará la titularidad de esta y la dificultad radicará en la localización de esa persona para que preste declaración en sede judicial en calidad de investigado. Si el número de cuenta facilitado pertenece a un tercero, se deberá dilucidar si ese tercero corresponde a una persona real o ficticia y, en el primer caso, si actuó en connivencia con el autor, lo que nos conduciría a cuestiones relativas a la autoría y participación en el delito.

La identificación del autor, para el caso de que los datos bancarios facilitados fueran falsos o pertenecientes a un tercero ajeno al fraude, debería realizarse a través de la investigación de la IP desde la que se emitió el anuncio en cuestión. En este punto, debemos indicar que también se suscitan problemas en la práctica. Bien es cierto que contamos con la nueva regulación, entre otras, de lo establecido en el artículo 588.ter de la Ley de Enjuiciamiento Criminal, específicamente el artículo 588.ter.k LEcrim y en el artículo 588.octies LEcrim, pero hemos de tener en cuenta las limitaciones temporales establecidas en este último («los datos se conservarán durante un período máximo de noventa días, prorrogables una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días»). Asimismo, debemos tener presente lo dispuesto en el artículo 5 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, según el cual «la obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores»; norma que debe ser interpretada a la luz de la Sentencia del Tribunal de Justicia de la Unión

y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información y que presentan por tanto, a los efectos de su investigación y/o enjuiciamiento singularidades y dificultades similares a las de los primeramente indicados. No obstante, esta circunstancia no debe llevarnos sin más a considerar que cualquier conducta delictiva en cuya ejecución se haga uso de las tecnologías de la información y la comunicación ha de incluirse en la categoría que nos ocupa».

Europea (Gran Sala) de 21 de diciembre de 2016.[10]

Como resulta sencillo deducir, en este tipo de estafa el autor de la misma ofrece el mismo producto a una pluralidad de personas, como decíamos, por lo que se cometerán tantos delitos de estafa como víctimas hayan contactado con el estafador. Quizás la respuesta penal que deberían tener tales supuestos sería la de su investigación y enjuiciamiento en un único procedimiento que permitiera comprender la dimensión real del ilícito, respuesta que no siempre se produce en la práctica donde el procedimiento se limita a un único delito, en la mayoría de los casos.

La dispersión geográfica de las víctimas es uno de los elementos que explican la dificultad para investigar este tipo de estafas de manera conjunta en un único procedimiento. La existencia de una pluralidad de víctimas en diferentes puntos de la geografía (sin contar con la posibilidad de que alguna de ellas pueda residir en el extranjero, circunstancia que añadiría nuevas dificultades en la investigación) implicaría la necesidad de realizar actuaciones judiciales en muchos casos mediante exhortos, lo que dilataría el procedimiento inevitablemente; si bien, esta dificultad podría verse mitigada con la declaración de complejidad de la causa en los términos del artículo 324 LEcrim.

En caso de investigarse y enjuiciarse en un único procedimiento una pluralidad de estafas, no existe óbice para considerar que se trataría de un delito continuado en los términos del artículo 74 CP: «El que, en ejecución de un plan preconcebido o aprovechando idéntica ocasión, realice una pluralidad de acciones u omisiones que ofendan a uno o varios sujetos e infrinjan el mismo precepto penal o preceptos de igual o semejante naturaleza».[11]

Cuestión distinta será ventilar la relación existente entre lo dispuesto en el artículo 74 CP y el subtipo agravado del artículo 250.1.5 CP (que «el valor de la defraudación supere los 50.000 euros o afecten a un elevado número de personas»).

El Acuerdo del Pleno no jurisdiccional del Tribunal Supremo de fecha 30 de octubre de 2007 estableció que «el delito continuado siempre se sanciona con la mitad superior de la pena. Cuando se trata de delitos patrimoniales la pena básica no se determina en atención a la infracción más grave, sino al perjuicio total causado. La regla primera, artículo 74.1 CP queda sin efecto cuando su aplicación fuera contraria a la prohibición de doble valoración».

Como ha venido entendiendo la jurisprudencia,[12] el delito continuado recoge el mayor contenido del injusto derivado de la constatación de una comisión sucesiva y reiterada de unas conductas agresivas a un mismo bien jurídico, bajo un dolo único y aprovechamiento de idénticas circunstancias. Es obvio que esa conducta, caracterizada por la concurrencia de los presupuestos del delito continuado, merece un mayor reproche penal. Desarrollando el citado Acuerdo del Pleno no jurisdiccional del Tribunal Supremo de fecha 30 de octubre de 2007, la jurisprudencia ha entendido, como se recogía ya en la STS 950/2007, de 13 de noviembre, que «cuando se trata de infracciones patrimoniales, la pena se impondrá teniendo en cuenta el perjuicio total causado conforme dispone el artículo 74.2 CP. De manera que si la suma de ese perjuicio es superior a 36.000 euros (actualmente 50.000 euros), la pena procedente es la prevista en el artículo 250.1.6º (actual artículo 250.1.5º CP) y si es inferior a esa cifra la del artículo 249 [...]. Cuando esa cifra (la relevante para incrementar la pena básica) se alcanza por la suma de las diferentes infracciones, acudir a la agravación del apartado 1 del artículo 74 vulneraría la prohibición de doble valoración de una misma circunstancia o de un mismo elemento, pues de un lado se ha tenido en cuenta para acudir al artículo 250.1.6ª CP (actual artículo 250.1.5º CP), con la consiguiente elevación de la pena [...] y de otro se valoraría para acudir al artículo 74.1 CP, agravándola nuevamente. Ello conduciría a determinar la pena conforme al perjuicio total causado pero sin que fuera preciso imponerla en su mitad superior, de forma que el Tribunal podría recorrer la pena en toda su extensión».

10. La STJUE (Gran Sala) de 21 de diciembre de 2016 ha declarado contrarios a la Carta Europea de Derechos Humanos, en concreto a sus artículos 7, 8, 11 y 52.1, regímenes de conservación preventiva de datos relativos a las comunicaciones basados, como nuestra Ley 25/2007, en la implementación de la Directiva 2006/22/CE, declarada inválida por la STJUE (Gran Sala) de 8 de abril de 2014.
11. Cuestión que ya fue tratada en la Consulta FGE 3/1999, de 17 de septiembre, sobre la pena que procede imponer a las infracciones penales continuadas de carácter patrimonial.
12. *Vid*. STS 950/2007, de 13 de noviembre; STS 226/2007, de 16 de marzo, entre otras.

En relación con el delito masa, como modalidad agravada del delito continuado, con características específicas que le dotan de una autonomía y sustantividad propias,[13] cabe decir que, *a priori*, no hay obstáculo alguno para apreciarlo si concurren los elementos para ello; esto es, el dolo preconcebido (a diferencia del delito continuado, en el que se admite el dolo ocasional exteriorizador del que aprovecha idéntica ocasión) y los elementos propios del delito con sujeto pasivo masa, a saber, la notoria gravedad (gravedad económica) y la generalidad de personas (grupo numeroso de personas, incluso indeterminado, destinatarios de la actividad ilícita del autor). En este sentido, la STS 719/2010, de 20 de julio, afirmaba que «el llamado delito masa existe cuando un solo acto inicial del sujeto activo determina que acudan a él una pluralidad indeterminada de personas, como puede ocurrir en casos de publicidad engañosa».

Atendiendo a las características del tipo de estafas que analizamos, parece difícil encontrar en la práctica un supuesto de delito masa, pero ello no significa que sea totalmente imposible.

Otra de las cuestiones que deberíamos analizar es la posibilidad de que a través de las redes sociales se cometa una estafa piramidal;[14] partiendo de la utilización de las redes sociales como plataforma a través de la cual se pueda acceder al mayor número de potenciales víctimas.

3. Las redes sociales y otras posibles conductas típicas de contenido patrimonial

Cuando las conductas analizadas se incardinan en el seno de una organización o de un grupo criminal, más allá de los supuestos de mera coautoría, no habría inconveniente en calificar tales conductas conforme a lo dispuesto en el artículo 570.bis CP[15] (organización criminal) o en el artículo 570.ter CP[16] en su caso (grupo criminal).

Hasta el momento, nos hemos centrado en las estafas cometidas a través de redes sociales dedicadas a la compraventa de productos, generalmente, de segunda mano, pero ¿y a través de otras redes sociales como Instagram?

En este caso la estafa que denominamos «tipo» estaría dirigida, en su gran mayoría, a aquellas empresas que pretenderían publicitar sus productos por medio de los/las *influencers*.

No podemos dejar a un lado el hecho de que, evidentemente, no todo lo que se publica en Instagram corresponde con la realidad, es decir, una persona puede crearse un perfil y mostrar a través de sus fotografías y sus vídeos una vida que no es real, que no se corresponde con la suya, pero

13. *Vid*. STS de 10 de junio de 2014.
14. *Vid*. STS 324/2012 de 10 de mayo: «El autor de una estafa lesiona un deber de respeto de la organización del sujeto pasivo cuando le presenta una situación de hecho que induce a dicho sujeto a obtener falsas conclusiones. En los casos en que el actor propone a la víctima invertir en su negocio, le corresponde al actor ofrecer información veraz sobre los elementos básicos del negocio de que se trate, pues por la posición que ocupa en la relación, es el actor el único que dispone de esta información, que no es normativamente accesible a la víctima.
Por ello considera la mejor doctrina que debe apreciarse estafa cuando el actor propone a la víctima un negocio inexistente, revistiendo esta propuesta de una puesta en escena que la dota de verosimilitud, y obteniendo así que la víctima le entregue el dinero solicitado, efectuando un desplazamiento patrimonial destinado supuestamente a invertir en el negocio del actor, y recibir el beneficio correspondiente, cuando en realidad la intención del actor es apropiarse directamente del dinero recibido, sin invertirlo en negocio alguno, con notorio perjuicio para la víctima.
Esto es lo que ha sucedido en el caso actual, en el que el recurrente ofrecía a los perjudicados invertir en su negocio elevadas sumas de dinero, a cambio de un interés importante, aparentando solvencia mediante la constitución de una entidad mercantil de inversiones, realizando su oferta con la garantía de un pagaré que supuestamente garantizaba la devolución íntegra del dinero y abonando durante un corto tiempo los intereses prometidos, lo que servía de anzuelo para captar nuevos clientes, con cuyo capital se abonaban los intereses. Este modelo piramidal de estafa conduce necesariamente a la frustración del negocio prometido, pues en la medida que se incrementa el capital recibido, aumentan exponencialmente las necesidades de nuevos ingresos para abonar los intereses, hasta que el actor cesa en el pago de los intereses y se apropia definitivamente de los capitales fraudulentamente recibidos».
15. El artículo 570.bis CP define la organización criminal como «la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se reparten diversas tareas o funciones con el fin de cometer delitos».
16. El artículo 570.ter CP define el grupo criminal como «la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo 570.bis CP, tengan por finalidad o por objeto la perpetración concertada de delitos».

que precisamente esa vida publicitada, los miles de seguidores que pueden acceder a ese perfil y seguirlo, pueda interesar a determinadas empresas que quieran vincular sus productos, y por tanto publicitarlos, con ese estilo de vida, todo ello a cambio de la correspondiente contraprestación económica. El hecho de que la «vida exhibida» no sea real no constituye, *a priori*, un elemento determinante para concluir que podríamos estar ante una estafa. El anunciante lo que pretende es que sus productos lleguen al mayor número de consumidores potenciales y, en este sentido, su objetivo se cumple siempre y cuando los seguidores de la cuenta en cuestión correspondan a personas reales, ajenas a la realidad de la vida del *influencer*. La respuesta cambia si ese número elevado de seguidores que atrae al anunciante son falsos, comprados, no son personas reales, sino simples perfiles inactivos. En este supuesto, sí podríamos sostener que estaríamos ante una estafa. El/la *influencer* hizo creer al anunciante que efectivamente lo era, que tenía miles de seguidores y mediante ese engaño se generó error en aquel que determinó el desplazamiento patrimonial en su perjuicio. El mismo esquema y la misma respuesta obtendrá si lo analizado son las cuentas de YouTube; dependerá si las visitas recibidas son ciertas o no.

A través de las redes sociales podrán cometerse otros delitos de contenido patrimonial, como los delitos contra la propiedad intelectual e industrial (arts. 270 a 277 CP)[17] o los delitos relativos a la publicidad engañosa (art. 282 CP),[18] que encontrarían en ellas un medio en el que desarrollar su actividad de forma extraordinariamente eficaz, si bien su análisis excede con creces el objeto de este trabajo.

No podía finalizar el presente trabajo sin referirme a una conducta que, sin ser propiamente un delito de contenido patrimonial, prolifera en las redes sociales y plantea interesantes problemas concursales (que por razones obvias no entraré a estudiar en este trabajo); me refiero a la comercialización y venta de medicamentos (falsificados en su mayoría, lo que nos remitiría a los delitos contra la propiedad industrial, así como al delito de publicidad engañosa) a través de las redes sociales (mención aparte merecerían los supuestos de ofertas a través de las redes sociales de drogas tóxicas, estupefacientes o sustancias psicotrópicas, sustancias dopantes). Las redes sociales constituyen la plataforma que permite que el sujeto activo acceda al mayor número de personas posibles. El artículo 361 CP tipifica la conducta del que «fabrique, importe, exporte, suministre, intermedie, comercialice, ofrezca o ponga en el mercado, o almacene con estas finalidades, medicamentos, incluidos los de uso humano y veterinario, así como los medicamentos en investigación, que carezcan de la necesaria autorización exigida por la ley, o productos sanitarios que no dispongan de los documentos de conformidad exigidos por las disposiciones de carácter general, o que estuvieran deteriorados, caducados o incumplieran las exigencias técnicas relativas a su composición, estabilidad y eficacia, y con ello se genere un riesgo para la vida o la salud de las personas».

El artículo 13.d del Convenio del Consejo de Europa sobre la falsificación de productos médicos y delitos similares que supongan una amenaza para la salud pública, hecho en Moscú el 28 de octubre de 2011 (Medicrime),[19] define como una circunstancia agravante de los delitos relativos a la falsificación de medicamentos, que «los delitos de suministro y oferta de suministro se hubiesen cometido recurriendo a medios de difusión a gran escala, tales como los sistemas informáticos, y en particular internet».

4. Conclusiones

Comenzamos el presente trabajo fijando conceptos y centrando nuestra atención en las estafas cometidas a través de las redes sociales; en los términos analizados, concluimos que no son estafas informáticas, sino comunes.

17. El artículo 270.2 CP castiga «a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios».
18. El artículo 282 CP sanciona a «los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos».
19. Ratificado por España y publicado el Instrumento de ratificación en el BOE de 30 de noviembre de 2015.

El tipo de estafa analizado conlleva problemas prácticos en su investigación, desde la dispersión geográfica de las víctimas, la posible impunidad de determinadas conductas ante la escasa cuantía del fraude, hasta la dificultad para identificar y localizar al autor de tales hechos; cabría la calificación como delito continuado y en teoría como delito masa, aunque resultará difícil encontrarlo en la práctica por sus propias características.

Asimismo, las estafas estudiadas no serían los únicos delitos de contenido patrimonial que podrían ser cometidos a través de las redes sociales, como se han apuntado, resultando interesantes problemas concursales en algunos supuestos, que exceden del presente trabajo.

Como hemos visto, las redes sociales, en los supuestos estudiados, no constituyen elementos definitorios de los delitos analizados, permiten facilitar su comisión, constituyen la plataforma para la toma de contacto entre el sujeto activo y el sujeto pasivo, dificultan, en ocasiones, su investigación, pero ello tampoco debe llevarnos a la demonización de las mismas. Son nuevas herramientas de las que disponemos los humanos y, de la misma forma que debemos aprender a utilizarlas, el ordenamiento jurídico deberá ir dando respuesta a los problemas que vayan planteándose en la práctica.

Bibliografía

REY HUIDOBRO, L. F. (2013). «La estafa informática: relevancia penal del *phising* y el *pharming*», *La Ley Penal,* n. 101.

VELASCO NÚÑEZ, E. (2008). «Estafa informática y banda organizada. *Phising*, *pharming*, *smishing* y "muleros"». *La Ley Penal,* n.º 49.

PONCE IDATZIA, I. (2012) «Monográfico Redes Sociales». Observatorio Tecnológico. Ministerio de Educación, Cultura y Deporte.

Cita recomendada

LÓPEZ PESQUERA, Beatriz (2018). «El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 42-51. UOC [Fecha de consulta: dd/mm/aa]
<http://dx.doi.org/10.7238/idp.v0i27.3150>

Sobre la autora
Beatriz López Pesquera
blopezpesq@uoc.edu

Fiscal de la Audiencia Provincial de Barcelona
Profesora colaboradora de la UOC

UOC
Av. Carl Friedrich Gauss, 5
08860 Castelldefels