
La estafa informática

PID_00267795

Alfonso Galán Muñoz

Tiempo mínimo de dedicación recomendado: 3 horas



**Alfonso Galán Muñoz**

Profesor titular de Derecho penal de la Universidad Pablo de Olavide, doctor en Derecho y becario Formación de Profesorado Universitario (FPU) del Ministerio de Educación, de la Fundación Alexander von Humboldt y del Servicio Alemán de Intercambio Académico (DAAD). Ha realizado numerosas estancias de investigación en las universidades alemanas de Friburgo, Múnich, Tubinga y Berlín. Es experto en criminalidad informática y económica, temas a los que ha dedicado numerosas publicaciones, tanto nacionales como internacionales. Es investigador principal y miembro de varios proyectos de investigación nacionales y autonómicos, y responsable del Grupo PAIDI SEJ-571: Grupo de Investigación sobre el Sistema Penal y Criminología (SISPECRIM). También es el director del máster de Criminología y ciencias forenses de la Universidad Pablo de Olavide.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Maria Tamarit Sumalla (2019)

Primera edición: septiembre 2019
© Alfonso Galán Muñoz
Todos los derechos reservados
© de esta edición, FUOC, 2019
Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea este eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares de los derechos.

Índice

Introducción.....	5
Objetivos.....	7
1. El tipo básico del delito de estafa informática.....	9
1.1. Bien jurídico protegido	9
1.2. Tipo objetivo	10
1.2.1. Conducta típica	10
1.2.2. La producción de una transferencia no consentida de activos patrimoniales	12
1.3. Tipo subjetivo	16
2. Penalidad.....	18
3. La delimitación de la estafa informática de otras conductas afines.....	22
4. Disposiciones comunes.....	27
Ejercicios de autoevaluación.....	29
Solucionario.....	31
Bibliografía.....	32

Introducción

Pese a lo que mucha gente piensa, los primeros ataques informáticos que llamaron la atención del legislador penal no fueron ni los daños informáticos, ni los accesos ilegítimos a dicha clase de sistemas. Los primeros en recabar su atención fueron los abusos que se realizan mediante el uso de dichas tecnologías y que tratan de obtener un enriquecimiento patrimonial a costa de la consecución de una transferencia de activos que determina la merma patrimonial de un tercero.

Este tipo de ataques empezaron a proliferar ya en los años setenta y principios de los ochenta en los países más desarrollados, como consecuencia de la imparable expansión del uso de las nuevas tecnologías tanto en las Administraciones públicas como en las grandes empresas. Casi todos ellos eran ataques en los que quienes los cometían se aprovechaban del acceso que tenían a dichos sistemas para conseguir que se les transfirieran a sus cuentas corrientes, de forma automatizada y sin autorización, cantidades significativas de dinero, lo que ocasionaba enormes pérdidas a las entidades y personas afectadas, sin que los tipos delictivos vigentes en aquel momento pudiesen castigar su ejecución.

Por ejemplo, supuestos como los del *Kindergeld* en Alemania, donde un trabajador de la Administración de un *Land* se dedicó a introducir los datos de supuestos e inexistentes nuevos nacidos en el sistema con el fin de que se les adjudicasen las ayudas que estaban previstas para fomentar la natalidad, pero que en realidad eran siempre transferidas a una cuenta a su nombre, o las del fraude de seguros que realizó en Estados Unidos el trabajador de una gran compañía aseguradora que introdujo en el sistema informático de dicha entidad siniestros inexistentes, cuyas indemnizaciones se transferían automáticamente a su cuenta, pusieron sobre aviso de la existencia de unas conductas abusivas que no tenían un encaje claro en ninguno de los delitos tradicionalmente dedicados a proteger el patrimonio.

Se constató, en concreto, que mientras el delito de hurto no podía aplicarse a esta serie de supuestos como consecuencia de que las referidas conductas no suponían la realización de ningún acto de sustracción de cosas muebles ajenas, sino la transferencia del activo representado mediante una anotación informática en cuenta, tampoco la estafa parecía poder responder a dichas conductas, dado que las transferencias se realizaban de forma automatizada y **sin que mediase engaño alguno realizado frente a un tercero que realizase un acto de disposición patrimonial, inducido por error, tal y como esta figura requería**. En esta misma línea, también quedó claro que la posición que ostentaban los autores de este tipo de actuaciones no siempre permitía apreciar aquel abuso de confianza que caracteriza al legítimo poseedor de una cosa ajena que se apodera de ella y que, al hacerlo, comete el delito de apropiación indebida.

Existía, por tanto, una innegable laguna de punibilidad en relación con estos casos, lo que determinó que no tardasen en aparecer propuestas tendentes a solventarla.

Precisamente, entre estas propuestas destacó una procedente de la doctrina alemana, que consideraba que este tipo de actuaciones, si bien no eran susceptibles de ser castigadas como estafas, dado que no suponían la realización de una conducta interpersonal comunicativa engañosa y generadora de un acto voluntario de disposición patrimonial ajeno, que define y caracteriza a dicho delito, sí que presentaba similitudes estructurales con esta figura, lo que llevó a que se crease el delito contenido en el §263.a del Código penal alemán. El **delito de *Computerbetrug* o estafa informática.**

No debe pasarse por alto este claro precedente internacional a la hora de entender el origen del delito que incorporó el Código penal de 1995 a nuestro ordenamiento, en aquel momento en el artículo 248.2 CP, que está actualmente vigente en el artículo 248.2.a CP y que tradicionalmente ha sido denominado como «estafa informática», pese a que, como veremos, son muchas las razones que alejan a dicha figura de la verdadera estafa.

En el presente módulo trataremos los principales elementos configuradores de esta figura.

Lectura recomendada

Sobre la situación y argumentos doctrinales que llevaron a la aparición del delito de estafa informática, resulta interesante leer la obra siguiente:

U. Sieber (1980). *Computerkriminalität und Strafrecht*. Colonia: Heyman.

Objetivos

Después de trabajar los materiales que componen este módulo didáctico, el estudiante podrá alcanzar los siguientes objetivos:

1. Conocer y comprender los elementos configuradores del delito de estafa informática.
2. Diferenciar el delito de estafa informática del de estafa tradicional.
3. Diferenciar el delito de estafa informática de otras figuras a las que está asimilada a efectos de pena.
4. Conocer y ser capaz de valorar jurídicopenalmente las más frecuentes formas de aparición del delito de estafa informática.
5. Comprender y saber aplicar los criterios que se utilizan para graduar la pena aplicable a los responsables de estafas informáticas.
6. Resolver los problemas concursales que pueden generarse en los casos de comisión de estafas informáticas.
7. Diferenciar el delito relativo a la creación o mera posesión de programas específicamente destinados a cometer estafas y los meros actos preparatorios punibles de estafas informáticas.

1. El tipo básico del delito de estafa informática

1.1. Bien jurídico protegido

Como suele suceder con los delitos informáticos, también en la estafa informática se discutió por parte de la doctrina si nos encontrábamos ante una figura protectora de un bien jurídico tradicional y de naturaleza puramente **patrimonial individual** o si, por el contrario, como algunos defendían (Rovira del Canto, 2002), estábamos ante una que tutelaba, junto a dicho valor o incluso en lugar del mismo, un interés de naturaleza supraindividual que vendría delimitado por la referencia al siempre cuestionado y cuestionable valor de la «seguridad de los sistemas informáticos».

Como ya tuvimos ocasión de exponer con mucha mayor extensión (Galán Muñoz, 2005), a nuestro juicio, resulta imposible mantener que el delito aquí analizado trate de proteger algo que no sea el patrimonio individual de la persona afectada por su comisión.

Muchos son los indicadores de la naturaleza marcadamente patrimonial individual de este delito. No es solo su ubicación sistemática (no olvidemos que está entre «los delitos contra el patrimonio y el orden socioeconómico») o que su tipo aluda expresamente a la necesidad de que se ocasione una transferencia de activos patrimoniales para apreciar su realización. Es que, además, como tendremos ocasión de comprobar, mientras su tipo no alude ni exige en modo alguno la afectación de más de un sistema informático para ser apreciado, sí que da una clara función excluyente de la tipicidad al consentimiento del titular del activo patrimonial transferido, algo que evidentemente resulta imposible de compatibilizar con la pretendida concepción supraindividual de su bien jurídico.

Si a todo ello le añadimos que, como veremos, la pena que se habría de imponer a su autor va a quedar siempre condicionada por la gravedad de la lesión patrimonial producida y no por la afectación del sistema o de los sistemas informáticos, no quedará más remedio que considerar que será precisamente la afectación de este valor individual (el **patrimonio**), y no el de la siempre difusa e indeterminada «**seguridad**» de tales sistemas, la que definirá la anti-juridicidad material del injusto propio de este delito, determinando así que dicho interés tenga que ser considerado como su bien jurídico protegido.

1.2. Tipo objetivo

El vigente artículo 248.2.a CP establece que se castigará como reos de estafa a quienes, «con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro».

1.2.1. Conducta típica

Estamos ante un delito común que puede ser cometido por cualquier persona y que, aparentemente, delimita su conducta típica aludiendo a dos posibles actuaciones de forma alternativa. Por una parte, estaría la **manipulación informática**, mientras que, por otra, estaría el **artificio semejante**.

Algunos autores, en un intento por mantener la cercanía estructural entre este delito y el tradicional de estafa, consideraban que solo tendrían cabida en el concepto de **manipulación informática** aquellas actuaciones realizadas sobre sistemas informáticos que provocasen que los procesamientos de datos efectuados en ellos llevasen a un resultado objetivamente defectuoso o erróneo, del mismo modo que el engaño de la estafa tiene que llevar a la producción de un erróneo acto de disposición patrimonial en aquel que sufre su engaño típico.

El principal problema al que se enfrentaba esta propuesta se planteaba a la hora de delimitar cuál habría de ser el referente al que habría que atender a la hora de valorar cuándo el resultado emitido por el sistema sería incorrecto o erróneo. En ese sentido, resulta obvio que, dado que los ordenadores se limitan a procesar los datos que se les introducen, atendiendo a las instrucciones que contemplan sus programas, emiten siempre resultados que son acordes y correctos conforme a lo que tienen programado, incluso aunque tales resultados hubiesen sido producto de la introducción de datos falsos o a una manipulación del programa utilizado para procesarlos. El parámetro para determinar cuándo un resultado es o no correcto no puede definirse, por tanto, como algunos pretendían, atendiendo al funcionamiento normal o anormal del sistema.

A nuestro modo de ver, resulta mucho más adecuado entender que cuando el legislador alude a la manipulación informática en este tipo delictivo, lo hace con la intención de que se castigue cualquier conducta realizada sobre dichos sistemas que dé lugar no a un erróneo procesamiento de datos, sino al resultado que el propio delito trata de impedir: **la producción de una transferencia no consentida de activos patrimoniales**.

De esta forma, se tendrá que considerar que tienen cabida en el concepto de manipulación informática cualquier introducción de datos (*input*), cualquier conducta que incida en el programa o en el funcionamiento del mismo durante el procesamiento de los datos (*tratamiento*) o cualquier actuación que alterase directamente el resultado de dicho procesamiento (*output*), siempre y cuando tales actuaciones resulten adecuadas precisamente para provocar la transferencia de activos patrimoniales que pretende evitar y castigar este delito. Es decir, cualquier utilización del sistema que sea susceptible de producir una transferencia no consentida de activos patrimoniales.

No obstante, todavía queda por definir qué conductas podrían tener encaje en la otra modalidad comisiva de esta figura. Es decir, qué conductas podrían ser consideradas y castigadas como formas de «**artificios semejantes**» a la referida manipulación.

Lo primero que hay que señalar a este respecto es que, una vez que se ha afirmado que cualquier conducta realizada sobre sistemas informáticos susceptible de producir transferencias no consentidas de activos patrimoniales debe ser considerada como una verdadera manipulación informática, parece obvio que no existirá ya ningún uso o abuso imaginable de alguno de estos sistemas que pueda tener como un mero «artificio semejante» a dicha modalidad, dado que todos serán subsumibles en la de manipulación propiamente dicha.

Posiblemente por ello, una parte de nuestra doctrina y algunas sentencias iniciales optaron por entender que cuando el legislador hablaba de la utilización de artificios semejantes a la manipulación informática, no estaba aludiendo a «artificios informáticos semejantes a dichas manipulaciones», sino a artificios que, precisamente por el hecho de no recaer sobre sistemas informáticos, no tendrían cabida en la manipulación que el artículo 248.2.a CP contempla como primera modalidad comisiva y podrían ser castigadas por la segunda. Es decir, estaba aludiendo a «artificios semejantes a las manipulaciones no informáticas» (Almela Vich, 1998), postura que les llevó a entender, por ejemplo, que esta sería precisamente la modalidad comisiva que permitiría que este delito castigase los abusos contra aparatos automáticos que se efectuasen manipulando su parte mecánica y no la informática o la digital del aparato en cuestión (véase, por ejemplo, SAP Lugo, de 9 de enero de 1998).

El problema de esta propuesta se deriva, a nuestro modo de ver, del hecho de que, si se interpreta, como la misma pretende, que el artificio semejante del que habla el artículo 248.2.a CP está referido al uso o, mejor dicho, al abuso de este tipo de mecanismos automatizados no informáticos, nos encontraríamos con que se estaría utilizando esta segunda modalidad para castigar unas actuaciones que ni se parecen a las que sanciona la conducta de manipulación en tener un carácter informático, ni tampoco lo hacen por ser similares en su

forma de realización, ya que poco o nada tiene que ver manipular o forzar el mecanismo físico, por ejemplo, de un aparato expendedor para que entregue un producto sin pagar por él, con manipular un sistema informático para que dé lugar a una transferencia de activos.

Precisamente por ello, hace ya tiempo que dijimos que, en realidad, la enorme extensión que tiene la modalidad comisiva referida a la manipulación informática ha determinado que la relativa al artificio semejante quede completamente carente de contenido, ya que mientras que no puede castigar ningún artificio informático análogo a la manipulación que no esté ya castigado en la primera modalidad comisiva, tampoco podrá sancionar ningún artificio no informático que se asemeje realmente a dicha manipulación sin infringir el principio de legalidad. Habrá que entender, por tanto, que es una referencia normativa nula y carente de cualquier clase de posible aplicabilidad práctica (Galán Muñoz, 2005).

1.2.2. La producción de una transferencia no consentida de activos patrimoniales

La realización de las conductas que analizamos en el apartado «Conducta típica» solo dará lugar a la consumación del delito de estafa informática cuando se llegue a materializar en la producción de una **transferencia no consentida** de activos patrimoniales.

Como ya hemos señalado, este elemento típico se convierte en el referente fundamental del tipo de injusto de la denominada *estafa informática*, ya que además de definir su resultado consumativo, poniendo así de manifiesto su marcado carácter patrimonial individual, resulta también un referente fundamental, como acabamos de ver, a la hora de concretar qué usos o abusos de sistemas informáticos van a poder tener cabida entre las manipulaciones informáticas que castiga esta figura, puesto que solo aquellos que resulten idóneos para producir dicho resultado podrán ser típicos de esta figura delictiva.

Por **transferencia** de activos patrimoniales habrá que entender el traspaso de un valor patrimonial de cualquier naturaleza que se produzca a resultas de la manipulación informática previamente realizada, esto es, el cambio de la titularidad del activo patrimonial afectado.

No obstante, dicho traspaso o cambio de titularidad habrá de producirse, además, **de forma no consentida**.

La exigencia de este elemento típico lleva a que la concurrencia del consentimiento referido a la transferencia actúe como causa determinante de la exclusión de la tipicidad de su efectiva producción, lo que nos obliga a tener que determinar **quién será el sujeto** que podrá emitir dicho consentimiento

y también **qué requisitos** habrá de tener su expresión acorde con la transferencia producida para poder determinar la atipicidad de la misma o incluso, como veremos, de la actividad realizada.

Por lo que se refiere a la primera cuestión, parece obvio que si el referente del consentimiento del que venimos hablando es la transferencia de activos patrimoniales, quien habrá y podrá emitirlo será aquel que tiene la capacidad y está legitimado para realizar el trasvase de patrimonio que esta determinaría. Es decir, el titular de los activos patrimoniales transferidos o aquellos otros sujetos que estuviesen legitimados o autorizados por aquel a realizar dicho tipo de actuaciones con respecto a su patrimonio (por ejemplo, un representante, un administrador, etc.), sujetos que, por otra parte, si se exceden, al autorizar o realizar la transferencia, del poder que el propietario les había otorgado para poder disponer de su patrimonio, no cometerán este delito, sino los de administración desleal o de apropiación indebida de los artículos 252 y 253 CP, dependiendo de si se habían excedido intensiva o extensivamente en el uso de dichos poderes (Núñez Castaño, 2017).

En consecuencia, habrá que entender que lo que permite apreciar el ataque que define el injusto del delito en cuestión es la ausencia del consentimiento del titular del patrimonio afectado por la transferencia que su realización vendría a ocasionar y no la del otorgado por el mero titular del sistema empleado. Esto, además de volver a acreditar el carácter eminentemente patrimonial de la figura de la que venimos hablando, obliga a analizar la posible relevancia penal de los meros accesos o usos no autorizados o consentidos de dichos sistemas, atendiendo a otros delitos, como el de acceso no autorizado a sistemas informáticos del artículo 197 bis.1 CP o, incluso, el de abuso de sistemas de acceso condicional del artículo 286.4 CP, y no a lo establecido en el artículo del que nos venimos ocupando.

Por otra parte, en relación con los requisitos que ha de tener el consentimiento en cuestión, hay que señalar que lo que el delito del artículo 248.2.a CP requiere para excluir la relevancia penal de la transferencia producida es que concurra el consentimiento de alguno de los referidos sujetos antes de que esta se llegue a materializar. Es decir, que no esté ausente cuando la transferencia se produzca. Esta exigencia asemeja notablemente la configuración típica de la figura ahora analizada a la de un delito patrimonial de enriquecimiento que poco tiene que ver con la estafa. La asemeja, en concreto, a la propia del delito de hurto, figura patrimonial de enriquecimiento que, como es sabido, se caracteriza precisamente por realizarse sin el consentimiento del ofendido por su ejecución.

De hecho, el delito ahora analizado, al igual que sucede con dicha figura tradicional de apoderamiento, no exige que el titular se oponga de forma expresa al trasvase patrimonial producido. Ni siquiera que lo conozca. Basta con que

no lo consienta, algo que evidentemente se dará si la transferencia se hace sin que haya conocido su producción, dado que difícilmente va a poder consentir algo que desconoce.

Por otra parte, en la estafa informática, como también sucede en el hurto, el consentimiento podrá emitirse tanto de forma expresa como tácita, y su presencia se podrá apreciar incluso cuando se haya emitido como consecuencia de que quien consintió fue engañado para hacerlo, situación que llevará a que no podamos ya decir que la transferencia se produjo «sin consentimiento», sino a que hayamos de afirmar que lo hizo con el consentimiento viciado, pero consentimiento al fin y al cabo, que distingue y separa el delito de la mal llamada «estafa informática» que castiga el artículo 248.2.a de nuestro Código penal del verdadero delito de estafa del artículo 248.1 CP, como también lo hace con esta última figura respecto a la tradicional de hurto.

Lo decisivo aquí, por tanto, es que no haya una voluntad acorde al traspase patrimonial producido, emitida por quien podía hacerlo, ya que la presencia de dicha voluntad, tanto si es expresada de forma meramente tácita como si se emite viciada por error, determinará que no se pueda atribuir el perjuicio patrimonial derivado de la transferencia producida a la manipulación previamente realizada, sino a la actuación que realizó aquel que la autorizó. Ello, evidentemente, tendrá importantes efectos típicos, aunque no siempre determinará la atipicidad de la conducta realizada.

De hecho, a nuestro modo de ver, solo si el titular o el legitimado respecto al patrimonio ajeno emite su consentimiento antes de que el tercero utilice el ordenador para realizar la transferencia, habrá que entender que su manifestación de voluntad determinará que ni siquiera se pueda hablar de la realización de una de las manipulaciones informáticas que abrirían las puertas a la apreciación de la tentativa de este delito. De lo contrario, es decir, si lo hace después de que el tercero ya hubiese utilizado el sistema informático en cuestión de forma idónea para producir la transferencia inicialmente no consentida por su parte, su voluntad ya no podrá impedir que se pueda y se deba apreciar la realización de la manipulación típica de esta figura. En realidad, lo que dicho consentimiento determinará será, simple y llanamente, que no se pueda imputar a dicha actuación ilícita previamente realizada la lesión producida a resultas de la posteriormente consentida transferencia, algo que, si bien cerrará las puertas a que se pueda apreciar el injusto completo o consumado de este delito, en modo alguno llevará a que no se pueda y se deba responsabilizar al manipulador por la tentativa realizada.

Así, pues, habrá que entender que la concurrencia del consentimiento referido a la transferencia no siempre llevará a la atipicidad del uso de sistemas informáticos cometido para generarla. De hecho, el consentimiento solo determinará la completa atipicidad de la conducta realizada cuando se emita antes de que se realice la actuación idónea para producir el trasvase patrimonial propio de la transferencia de activos de la que habla la estafa informática, lo que llevará a que no nos encontremos ante una manipulación informática de este delito, por lo que la actuación realizada quedará en la más absoluta tipicidad. El emitido tras la realización de la referida manipulación, sin embargo, tan solo romperá la imputación objetiva entre dicha conducta y el resultado lesivo propio de este delito, lo que impedirá apreciar la consumación de este delito, pero en modo alguno impedirá que se pueda apreciar su realización en grado de tentativa.

No obstante, una vez que se pone de manifiesto que las transferencias de activos de las que habla el delito aquí analizado han de ser realizadas sin intervención de la voluntad humana de ningún tercero, para que no se rompa la necesaria relación de imputación objetiva entre la acción (la manipulación informática) y el resultado típico de su injusto, se deja meridianamente claro que el trasvase de la titularidad de los activos protegidos por este delito necesariamente deberá derivarse de forma directa del procesamiento de datos realizado y no de actuaciones posteriores o simultáneas de terceros.

No bastará entonces con que la actuación realizada dé lugar simplemente a un cambio en un documento o en un registro informático que pueda llevar a que un tercero pueda posteriormente realizar un acto dispositivo y voluntario que genere la efectiva traslación de la titularidad del bien representado, ya que ello determinaría que el traspaso producido se debiese atribuir a dicho acto de disposición errado y no a la manipulación previamente efectuada. Para que tengamos el delito de estafa informática consumado, se requiere que el cambio del registro informático producto de la manipulación efectuada sea el que genere, directa e inmediatamente, la transferencia de la titularidad del activo en cuestión.

Efectiva traslación de la titularidad

No existe, por tanto, efectiva traslación informática del patrimonio ni delito de estafa informática en aquella conducta que realizaría el repartidor que, atendiendo a lo que ponía su listado de entrega, previamente manipulado por un tercero, le entrega algo que en realidad tendría que haber entregado a otro.

Esto, evidentemente, limitará el ámbito de aplicación y de protección de este delito a aquellos activos patrimoniales cuya titularidad esté contemplada en sistemas informáticos que los representen de tal forma que el cambio en la anotación o registro informático referido a los mismos en el sistema determine el automático cambio de su titularidad.

Así sucederá, por ejemplo, con los registros informáticos que se contienen en el sistema español de pagos interbancarios empleado para realizar las compensaciones de todas las operaciones, grandes o pequeñas, efectuadas entre las entidades bancarias o con las anotaciones en cuenta que representan los activos negociados en el mercado continuo bursátil, registros que otorgan la titularidad legal de los activos que representan a quien aparece en los mismos como tal, con lo que su modificación para atribuir la titularidad a un tercero, determina que produzca la automática y efectiva traslación del activo representado.

Finalmente, solo nos resta señalar que al requerirse que se alcance la efectiva transferencia de los activos afectados para poder apreciar la consumación de este delito patrimonial, se deja claramente establecido que solo podrá considerarse consumado el delito cuando se alcance la **efectiva pérdida del activo afectado por parte de su sujeto pasivo**, configurándose así esta figura como un claro ejemplo de delito de lesión cuya cuantía y magnitud, como veremos, tendrá una enorme importancia a efectos de determinar y graduar la pena que se habrá de aplicar a quienes lo cometan.

1.3. Tipo subjetivo

Nos encontramos ante una figura eminentemente **dolosa**, lo que, además de abrir las puertas al posible castigo de su tentativa, también llevará a que cualquier error, incluso el vencible, del sujeto que utilice un sistema informático referido a alguno de los elementos que configuran su tipo objetivo determine que su actuación quede al margen de la tipicidad de este delito.

No obstante, el injusto típico de esta figura no solo exige que se cometa de forma dolosa para poder ser apreciado sin exigir que se tenga que efectuar para cometer ningún delito de estafa posterior. También requiere que quien lo efectúe actúe con **ánimo de lucro** para poder ser castigado por él.

Se introduce así un especial elemento subjetivo en el injusto de este delito que lo convertirá en una figura de tendencia interna trascendente y de resultado cortado.

Por una parte, esto determina que no se pueda apreciar la realización de este delito cuando el sujeto que efectúe una utilización no autorizada de un sistema informático, no la lleve a cabo con la finalidad o pretensión de enriquecerse o enriquecer a otro gracias a la transferencia que su conducta podría ocasionar

Sistema español de pagos interbancarios

En concreto, el sistema español de pagos interbancarios está estructurado en torno a dos sistemas diferentes: El TARGET2-Banco de España, que se ocupa del procesamiento de grandes pagos y el Sistema Nacional de Compensación Electrónica (SNCE), para los pagos de pequeña cuantía. Por otra parte, respecto a la utilización de anotaciones en cuentas informáticas en el mercado continuo bursátil, véase lo establecido en los artículos 5 y 9 LMV.

sino solo con la de dañar al tercero afectado (piénsese, por ejemplo, en la actuación que realizaría aquel que borrara un activo patrimonial perteneciente a otro, sin intención alguna de transferírsele ni a él mismo ni a un tercero). Y, por otro lado, también llevará a que se pueda apreciar este delito en su modalidad consumada cuando el sujeto que use dicho sistema informático, lo haga para enriquecerse, incorporando a su patrimonio un activo patrimonial ajeno de forma no consentida, sin llegar, sin embargo, a conseguirlo, como sucedería, por ejemplo, si lograra que el activo representado en la cuenta bancaria de un tercero saliese o desapareciese de la misma, sin conseguir que se le ingresase en la suya porque su actuación fue detectada en el lapso que mediaba entre la realización de ambas anotaciones en cuenta, la de salida de activos de una y la de entrada en la otra.

2. Penalidad

La decisión legislativa de incluir el delito aquí analizado en el artículo 248 CP y de señalar que sus autores también serían «considerados como reos de estafas» determinará que se tenga que sancionar a quien lo cometa atendiendo al mismo régimen de penas que se prevé para este último delito. Es decir, para la estafa.

Esta cuestionable decisión legislativa, adoptada pese a que, como hemos visto, pocos son los elementos comunes que la figura aquí analizada tiene con dicho delito tradicional, dado que en la mal denominada estafa informática ni hay engaño, ni hay error, ni tampoco existe, ni puede existir, un acto de disposición patrimonial, dará lugar a que se den serios problemas a la hora de aplicar al delito aquí analizado muchas de las prescripciones relativas a las penas previstas para la estafa.

En cualquier caso, el primer efecto que tiene la asimilación a efectos de pena que ha establecido nuestro legislador entre el delito de estafa informática y el de estafa propiamente dicha llevará a que se tenga que aplicar al delito ahora analizado lo establecido en el artículo 249 CP, que afirma que «Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena, se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. **Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses**» (la negrita es nuestra).

Como se puede comprobar, este precepto, además de obligar al juez a determinar la pena aplicable al autor del referido delito teniendo en cuenta el importe de lo defraudado, también establece que si dicho importe no superase los 400 €, se le tenga que imponer una simple multa de hasta tres meses, con lo que se castigaría la estafa informática cometida como mero delito leve y se abrirían las puertas a que su realización pudiese dejar incluso sin sanción, atendiendo a lo establecido en los artículos 964.2.a y 963.1 LECrim.

No obstante, una vez que se supere dicha cuantía, además de poder aplicarle la pena «de seis meses a tres años» que establece el primer párrafo del artículo 249 CP para el tipo básico de este delito, también se abrirá la posibilidad de que se pueda llegar a castigar dicho sujeto por uno de los tipos cualificados que contempla el artículo 251 CP, algo que se presenta en determinados casos como difícil o incluso imposible de hacer, precisamente como consecuencia de que la estafa informática poco o nada tiene realmente de estafa.

Por ejemplo, resulta evidente que algunas circunstancias cualificadoras, como la contemplada en el artículo 250.1.6º CP, que incrementan la pena del autor de la estafa atendiendo al abuso de la credibilidad empresarial que hubiese realizado para cometerla, carecen de cualquier aplicabilidad práctica cuando se predicen con respecto a un delito, como es el de estafa informática, que se comete gracias a la realización de un abuso o de la manipulación de un aparato informático, y no mediante el engaño efectuado frente a un tercero.

Lo mismo sucede con el tipo cualificado referido a la denominada **estafa procesal**, cualificación que resulta difícilmente predicable con respecto a las conductas que venimos analizando.

De hecho, más bien parece que, de entre todas las circunstancias que pueden determinar la aplicación de la pena establecida por los tipos cualificados contemplados en el artículo 250 CP, son aquellas que aluden y se fundamentan en la magnitud del perjuicio o defraudación ocasionada a sus víctimas las que tendrán un mejor acomodo a la hora de ser aplicadas al delito de estafa informática, dado el carácter de delito de lesión patrimonial que, como hemos visto, tiene dicho delito.

Nos centraremos, por ello, en su estudio.

En concreto, tres son las posibles circunstancias cualificadoras que atienden a dicho referente:

- 1) La contemplada en el cuarto apartado del artículo 250.1 CP, que incrementa la pena cuando el delito cometido «revista especial gravedad, atendiendo a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia».
- 2) La contenida en el quinto apartado del referido artículo, que la incrementa cuando «el valor de la defraudación supere los 50.000 euros o afecte a un elevado número de personas».
- 3) La que se establece al final el artículo 250.2 CP, que contempla el tipo supracualificado de este delito y eleva la pena a aplicar a sus responsables hasta la de prisión de cuatro a ocho años «cuando el valor de la defraudación supere los 250.000 euros».

La primera, la contenida en el artículo 250.1 CP, permite incrementar la pena atendiendo a la gravedad que presente el delito teniendo en cuenta, además del criterio objetivo relativo a la **magnitud del perjuicio patrimonial producido**, otro elemento, en este caso de carácter subjetivo, que estará referido a la **situación económica** en que el delito en cuestión ha dejado a su víctima. Se pretende así que los jueces puedan incrementar la pena de aquellos delitos de estafas informáticas que, pese a no alcanzar las cuantías objetivas que se contemplan y delimitan los otros dos tipos cualificados anteriormente señalados, sí que supongan una merma del patrimonio de su víctima que incida de forma significativa en el desarrollo de su vida cotidiana o en la de sus familiares, ya que, evidentemente, no tendrá el mismo efecto sobre un sujeto si se le priva,

por ejemplo, de 1.000 € cuando tiene unos ingresos o un patrimonio que superan con creces dicha cuantía, que si dicha cantidad representa el importe íntegro de la pensión o el patrimonio que tenía para subsistir durante un mes.

No debe olvidarse, sin embargo, que para que se pueda apreciar este tipo cualificado, no bastará con que la conducta realizada lleve a que se produzca dicho efecto perjudicial valorado de forma objetiva-subjetiva. Además, será necesario que tal resultado haya sido abarcado por el dolo del sujeto que lo hubiese ocasionado, lo que evidentemente llevará a que si dicho sujeto no conociese, por ejemplo, la grave situación económica en que su actuación iba a dejar a la víctima a resultas de su conducta, no pueda ser ya sancionado con la pena prevista en este tipo, por más que objetivamente hubiese ocasionado tal resultado al referido sujeto.

Frente a esta cualificación, las otras dos se sustentan en una valoración puramente objetiva del perjuicio ocasionado y fijan unas cuantías a la hora de determinar cuándo se podrán apreciar. La primera, la contenida en el artículo 250.1.5º CP, permitirá apreciar este tipo cualificado, además de **cuando el delito afecte a un número elevado de personas** –lo que no es en modo alguno infrecuente en la realización de estafas informáticas, especialmente si se realizan, por ejemplo, sobre el programa que determina los pagos de un número elevado de personas (técnica de la «peluca» o el «salami»)–, también cuando la defraudación ocasionada **supere los 50.000 €**.

Técnica de la peluca

El ejemplo clásico de fraude mediante la técnica de la «peluca» o el «salami» fue aquel en que el operario de una entidad bancaria manipuló el programa que utilizaba dicha entidad para calcular los intereses de sus clientes con el fin de que se redondeasen a la baja, descontando tan solo unos céntimos de lo que le debería haber correspondido a cada uno, con el fin de transferir posteriormente el importe total rebajado a todos a la cuenta del manipulador, lo que, evidentemente, le reportó suculentos beneficios. De esta forma, la defraudación de pequeñas cuantías lleva a la producción de un gran beneficio, de modo análogo a como, «pelo a pelo», se hace una peluca, de ahí la denominación de este tipo de fraudes.

Nada más se requeriría para apreciar este tipo. Sería indiferente para el mismo, por ejemplo, el efecto que el perjuicio objetivamente producido, superior a los 50.000 €, tuviese sobre el afectado, con lo que daría igual si este era un humilde pensionista sin patrimonio que una gran entidad financiera con abundantes recursos.

Algo similar sucede con el **tipo supracualificado** contenido en el artículo 250.2 *in fine* CP. Su apreciación solo dependerá de que se superen los **250.000 € de perjuicio** ocasionado por el delito, algo que en los delitos de estafa informática no es en modo alguno infrecuente.

No lo es, entre otras razones, porque cuando un sujeto encuentra el método de utilizar un sistema de transferencia electrónica de activos para beneficiarse ilícitamente, normalmente emplea dicho método cuantas veces puede, lo que dará lugar a una repetición de manipulaciones delictivas que determinará que se tenga que apreciar el correspondiente delito continuado, que castigará tales actos de forma conjunta y teniendo en cuenta la cuantía del perjuicio total producido con su ejecución, y no por el que hubiese ocasionado cada una de las actuaciones realizadas de forma individualizada (art. 74.2 CP). Esto, evidentemente, permitirá, en no pocas ocasiones, que actuaciones que individualmente consideradas no alcanzarían las cuantías contempladas en los mencionados tipos cualificados del artículo 250 CP, las superen al valorarse de forma conjunta o continuada, algo que, como reiteradamente ha señalado el Tribunal Supremo, si bien permite el salto al tipo cualificado que produciría la valoración conjunta del perjuicio producido, cerrará la puerta a que se pueda aplicar al autor simultáneamente el incremento de pena que prevé de forma general el artículo 74.1 CP para los delitos continuados, para evitar así que la continuidad delictiva dé lugar a un doble incremento punitivo que infrinja el principio de *ne bis in idem*.

Sin embargo, el caso será diferente si una o varias de las conductas individuales que componen el delito continuado alcanzasen por sí solas la cuantía del tipo cualificado en cuestión (los 50.000 € o los 250.000 € anteriormente señalados). En este supuesto, la pena cualificada del correspondiente tipo cualificado se sustentaría sobre la base del perjuicio ocasionado por dicha actuación individual y no en la acumulación de perjuicios derivados de la continuidad, por lo que no existirá problema alguno para que se puedan aplicar acumulativamente el incremento de pena contemplado en dicho tipo y el establecido en el artículo 74.1 CP para los delitos continuados, al no suponer dicha doble subida de penas ninguna doble valoración de la continuidad delictiva concurrente.

Finalmente, resulta necesario diferenciar los casos de delito continuado de estafa informática de los que venimos hablando de aquellos otros en los que, habiendo una única manipulación informática, esta lleva como consecuencia del propio automatismo con que se usan los sistemas informáticos, a que se produzcan sucesivas y acumuladas transferencias patrimoniales no consentidas en perjuicio de tercero.

Así sucederá, por ejemplo, en el caso anteriormente comentado en el que se manipula el programa que calcula los intereses a abonar a los clientes de una entidad bancaria para redondearlos a la baja y transferir de forma automática lo restado a la cuenta del manipulador (técnica de la peluca). En estos supuestos, una sola manipulación será la que lleve a que se realicen transferencias no consentidas de forma periódica y repetida que incrementarán el perjuicio producido a sus víctimas, lo que, si bien intensificará la gravedad del delito cometido al aumentar la lesión producida por el mismo como consecuencia de la acumulación de los perjuicios producidos, en modo alguno permitirá que se pueda apreciar la realización de un delito continuado de estafa informática, y no uno solo, ya que no existe la pluralidad de actuaciones que, conforme establece el artículo 74.1 CP, requiere el delito continuado para poder ser apreciado.

Continuidad delictiva

Respecto al tratamiento de la continuidad delictiva en los delitos patrimoniales, véase lo establecido en el acuerdo del pleno no jurisdiccional de la Sala segunda del Tribunal Supremo de 30 de octubre de 2007.

3. La delimitación de la estafa informática de otras conductas afines

La imparable evolución legislativa ha llevado a que el legislador haya ido incluyendo otras figuras en el artículo 248 CP, junto a la estafa y a la estafa informática, cuyo estudio resulta fundamental para tener una correcta apreciación de cómo habrá que sancionar muchos de los casos de estafa informática realizados.

Así ha sucedido, por ejemplo, con el delito que introdujo la reforma realizada por la LO 5/2010 en el vigente apartado *c* del artículo 248.2 CP. Este precepto castiga como reo de estafa, es decir, con el régimen de penas anteriormente comentado, a «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».

La introducción de esta figura, la de **abuso de tarjetas de crédito o débito**, trataba de acabar con la controversia jurisprudencial existente hasta ese momento en relación con el modo de calificar las diferentes formas de abusos patrimoniales de enriquecimiento que se pueden realizar sobre todo mediante el uso de las tarjetas de crédito y débito. Estos abusos habían sido castigados, dependiendo de cómo se hubiesen cometido (ante personas, digitalmente, en cajeros, etc.), como hurto, robo, estafa o incluso mediante la apreciación del delito de estafa informática del que nos venimos ocupando (véase a este respecto, por ejemplo, Mata y Martín [2007] o Faraldo Cabana [2009]).

Para acabar con esta polémica jurisprudencial que también tuvo reflejo, como no podía ser de otro modo, en nuestra doctrina, nuestro legislador decidió crear esta nueva figura delictiva dirigida a castigar por igual todos estos abusos. De hecho, la intencionalmente amplia redacción de este precepto determina que esta figura sea la que se va a emplear, atendiendo al **principio de especialidad**, para castigar cualquier uso de las referidas tarjetas que se nos pueda ocurrir que, eso sí, dé lugar a una operación perjudicial para su titular o para un tercero.

Dará igual si la tarjeta ajena se usa en un supermercado para hacerse pasar por su titular y conseguir así la entrega de una mercancía por parte del empleado que, confiando en dicha falsa identidad, efectúa el cargo correspondiente a lo entregado en la tarjeta ajena, o si se emplea, lo que cada vez es más frecuente, para realizar una compra en línea mediante el uso de los datos identificadores de la tarjeta de un tercero (por ejemplo, número, fecha de caducidad y CVV), lo que determinará el cargo automático del precio de lo adquirido en la cuenta del legítimo titular de la tarjeta. Cualquiera de estas actuaciones tendrá cabida en este delito con tal de que dé lugar a una operación, habrá que entender

que financiera, que redunde en perjuicio de un tercero, ya sea este el titular de la tarjeta empleada o el propio comerciante o empresario que suministró su mercancía o servicio al uso realizado de la misma.

Con independencia de lo problemático que resulta desde el punto de vista de los **principios de proporcionalidad** (no debería valorarse ni castigarse igual el uso de tarjeta efectuado para engañar a otro, que el que se efectúa, por ejemplo, para sacar dinero de un cajero) y **de legalidad** (el tipo es tan amplio que resulta difícil de definir el tipo de operaciones que podría castigar, permitiendo incluso en apariencia que se castiguen igual las realizadas con ánimo de lucro y las que se efectúan con un mero dolo de perjudicar a otro), lo cierto es que, por lo que a nosotros nos interesa, esta figura atendiendo al **principio de especialidad** viene a extraer del ámbito de posible aplicación del delito de estafa informática a todas aquellas transferencias automáticas de activos patrimoniales no consentidas que se hayan conseguido realizar mediante el empleo, en un sistema informático, de tales tarjetas o de los datos obrantes en las mismas.

Así, pues, conductas tales como realizar una compra en línea de un billete de avión utilizando los datos obrantes en una tarjeta ajena, sin el consentimiento de su titular, habrán de ser castigadas conforme a lo establecido en el apartado c del artículo 248.2 CP y no por el delito de estafa informática, por más que no exista problema alguno para poder considerar que dicha actuación sería una de las manipulaciones informáticas que también podría castigar este delito.

Algo diferente sucede con otra de las figuras que nuestro artículo 248.2 CP viene a castigar como si fuesen estafas. La contemplada en la letra *b* de dicho artículo.

Fue la LO 15/2013 la que vino a introducir en el en aquel momento vigente artículo 248.3 CP, la figura que hoy aparece contemplada en el apartado *b* del vigente artículo 248.2 CP, donde se establece que también se considerarán como reos de estafa «Los que fabricaren, introdujeran, poseyeran o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo».

Pese a lo que en un primer momento se pudiese pensar, no estamos, como vamos a ver, ante un precepto que castigue una específica modalidad preparatoria del delito de estafa informática del que venimos hablando. Y no lo estamos, entre otras cosas, porque la figura contenida en el artículo 248.2.b CP no exige, para poder ser apreciada, que su actuación típica se efectúe con la intención o con el propósito de cometer un concreto y definido delito de estafa informática, lo que desvincula su injusto de aquel que contempla la figura que la precede, y convierte el delito ahora analizado, a nuestro modo de ver, en una figura completamente autónoma respecto de aquella.

De hecho, si nos fijamos, lo que aquí se castiga son una serie de conductas (**fabricar, introducir, facilitar** o simplemente **poseer**) que se convierten en típicas solo en la medida en que recaigan o estén referidas a un concreto objeto material que se considera especialmente peligroso: uno de los programas informáticos específicamente destinados a cometer estafas de los que habla este delito.

La comentada descripción de la conducta típica de este delito lo convierte en un tipo mixto alternativo que se podrá apreciar con la mera realización de cualquiera de las conductas descritas en su tipo, sin que la acumulación sucesiva de varias de ellas, realizadas por un mismo sujeto y con respecto a un mismo programa, pueda determinar que se le castigue por varios de estos delitos. Esto llevará, por ejemplo, a que si un sujeto fabricase uno de los programas de los que habla este tipo y posteriormente se lo facilitara a un tercero, se le tuviese que condenar por la realización de un único delito del artículo 248.2.b CP y no por dos, por más que *de facto* hubiese realizado dos de sus posibles conductas típicas.

No obstante, para que cualquiera de dichas actuaciones, ya sea la creación o fabricación, el suministro a un tercero, la introducción en el mercado o la mera posesión, pueda constituir este delito, habrá de ser llevada a cabo, tal y como ya apuntamos, sobre un objeto muy concreto: sobre programas específicamente destinados a cometer estafas.

Lo primero que llama la atención de la definición legal del medio comisivo típico de este delito es que está referido exclusivamente a programas. Esto es, al software que define la serie de instrucciones que seguirá un sistema informático a la hora de procesar los datos que se le introduzcan. Ningún otro instrumento podrá dar lugar a la apreciación de esta figura, por muy lesivo que pueda resultar para los patrimonios de terceros. Pero es que, además, por expreso mandato legislativo, solo darán lugar a la apreciación de este delito aquellos programas que estén «específicamente destinados a cometer estafas».

Esta exigencia legislativa resulta fundamental.

En primer lugar, porque pone de manifiesto que lo que definirá a estos programas será la aptitud o idoneidad objetiva del programa para cometer dichos delitos, y no el hecho de que puedan ser habilidosamente utilizados por algunos para cometerlos (Quintero Olivares, 2016). Se requiere, por tanto, que el programa presente una idoneidad *ex ante* para facilitar comisión de estafas, lo que convierte a esta figura en un delito de peligro hipotético que no podrá ser apreciado si el programa en cuestión no presenta la idoneidad que requiere su tipo de injusto.

Por otra parte y en segundo lugar, dicha exigencia también determina que no cualquier programa que resulte idóneo para cometer delitos de estafas pueda ser considerado como uno de los instrumentos cuya fabricación, introducción, facilitación o mera posesión dará lugar a la apreciación de esta figura. Por expresa exigencia legislativa, como hemos visto, solo podrá tenerse por tales aquellos que estén «**específicamente destinados**» a cometerlos.

Esta expresión normativa contrasta claramente con la que establecen otros preceptos de nuestro código que también persiguen conductas referidas a instrumentos informáticos peligrosos, pero los delimitan señalando que estos deben estar «primordialmente concebidos» para realizar una actuación ilícita. Esta divergencia legislativa nos lleva a pensar que, mientras estos últimos delitos, como veremos, podrán castigar conductas que recaigan sobre instrumentos que tengan utilidades adicionales y alternativas a las puramente delictivas, en el aquí analizado si el programa en cuestión tuviese cualquier otra utilidad, además de la defraudatoria, ya no se lo podría considerar como uno de aquellos programas típicos de este delito, ya que, por más que se pudiese entender que podría estar primordialmente destinado a cometer estafas, no se podría decir que estuviese específicamente destinado a hacerlo.

Esta figura se nos presenta pues como un delito de peligro hipotético que tan solo exige que se cometa de forma dolosa para poder ser apreciado, lo que, si bien no impide que venga a sancionar conductas que se mueven en el ámbito de lo meramente preparatorio con respecto a la posible comisión de futuros delitos de estafas informáticas, sí que llevará a que, como adelantamos, no se pueda entender que sancione meros actos preparatorios específicos de uno de esos delitos.

De hecho, a nuestro modo de ver, dado que el artículo 248.2 CP castiga con la misma pena al autor de este delito que a aquel que efectivamente realiza el delito de estafa informática y lo hace, además, exigiendo que el programa del que habla esté específicamente destinado a cometer estafas (en plural) y no una (en singular), parece que lo más lógico será considerar que nos encontramos ante un delito que solo se podrá apreciar cuando el programa que se analice a la luz de su tipo de injusto **resulte idóneo para poder cometer no una, sino un número enorme de estafas frente un número amplio e indeterminado de posibles sujetos pasivos**. Esto, además de justificar que el artículo 248.2 CP pueda castigar con la misma pena una mera conducta peligrosa para el patrimonio, como la contemplada en su letra *b*, y una efectivamente lesiva del mismo, como la que sanciona su apartado *a*, llevará a que se tenga que entender que cuando concurra en un mismo hecho la ejecución de ambos delitos, los dos tengan que entrar en concurso de delitos y no de leyes, dado que al castigar la figura ahora analizada, la puesta en peligro de un número enorme e indeterminado de bienes jurídicos patrimoniales individuales, su

Lectura complementaria

A. Galán Muñoz (2004). «El nuevo delito del artículo 248.3 CP: ¿Un adelantamiento desmedido de las barreras de protección penal del patrimonio?». *Revista LA LEY* (n.º 6037).

injusto nunca podrá llegar a ser absorbido de forma completa por la efectiva lesión patrimonial individual que castigase la estafa informática apreciada, por muy amplia e intensa que dicha lesión pudiese ser en cada caso concreto.

4. Disposiciones comunes

Existen toda una serie de disposiciones que resultan aplicables tanto a la estafa informática como al resto de delitos que hemos analizado en este módulo.

La primera es aquella que contiene el artículo 251 bis CP, que permite responsabilizar penalmente a las personas jurídicas por la comisión de estos delitos en caso de que concurran los requisitos establecidos en el artículo 31 bis CP.

Por otra parte, también resultan aplicables a todas estas figuras las disposiciones comunes contenidas en los artículos 268 y 269 CP.

La contemplada en el artículo 268 CP establece una excusa absolutoria que dejará exentos de penas, aunque seguirán siendo civilmente responsables, a «los cónyuges que no estuvieren separados legalmente o de hecho o en proceso judicial de separación, divorcio o nulidad de su matrimonio, y los ascendientes, descendientes y hermanos por naturaleza o por adopción, así como los afines en primer grado si viviesen juntos, por los delitos patrimoniales que se causaren entre sí, siempre que no concurra violencia o intimidación, o abuso de la vulnerabilidad de la víctima, ya sea por razón de edad o por tratarse de una persona con discapacidad».

Los efectos de dicha disposición sobre el delito de estafa informática son innegables, dado que al ser el mismo un delito patrimonial en el que no se requiere ni suele darse el uso de violencia, intimidación o de abusos de situaciones de superioridad, es, sin duda, una de las figuras en las que la concurrencia de las referidas relaciones parentales entre sus responsables y sus víctimas determinará que se tengan que dejar exentos de responsabilidad a los primeros.

Algo parecido sucederá con el delito de abuso de tarjetas contemplado en el artículo 248.2.c CP.

Sin embargo, a nuestro modo de ver, muy diferente será el caso del delito referido a los abusos de programas específicamente destinados a cometer estafas que castiga el artículo 248.2.b CP, dado que, al considerarse, como aquí se ha hecho, que dicha figura protege los intereses supraindividuales de todos los que se podrían ver afectados por la creación o distribución de dicha clase de programas, habrá que entender que nos encontramos ante un verdadero delito socioeconómico y no ante uno meramente patrimonial, que, consecuentemente, no entrará dentro del ámbito de aplicación de la excusa absolutoria de la que venimos hablando.

Finalmente, solo nos resta señalar que el artículo 269 de nuestro Código penal prevé el castigo de las formas de participación intentada con respecto a todos estos delitos. Esto es, de la **proposición**, de la **provocación** y de la **conspiración**, lo que, si bien ya resulta cuestionable en relación con unos delitos como los de estafa informática, meramente patrimoniales, aún lo es más cuando se aplica respecto al delito referido a los programas específicamente destinados a cometerlas que castiga el artículo 248.2.b CP, por cuanto al venir dicha figura a castigar meros actos preparatorios de delitos de estafa en general, si se castigasen los meros actos de proposición, provocación o conspiración de dicha figura, se estarían castigando lo que no dejaría de ser sino meros actos preparatorios de otros actos preparatorios, algo que, sin duda, supondría una desmedida y desproporcionada intervención penal.

Ejercicios de autoevaluación

1. El delito de estafa informática...

- a) castiga como estafa conductas engañosas que se realizan frente a un ordenador.
- b) se castiga con la misma pena que la estafa porque su injusto presenta una estructura similar al de este delito.
- c) sanciona como si fueran estafas actuaciones que, a diferencia de las sancionadas por dicho delito, ni requieren de la comisión de un engaño, ni de la producción de un erróneo acto de disposición patrimonial.
- d) permite castigar los abusos patrimoniales que se realicen manipulando la parte mecánica en aparatos automáticos.

2. Se incardinan dentro de las manipulaciones informáticas castigadas por el delito de estafa informática...

- a) solo las actuaciones de introducción de datos falsos en el sistema informático (*input*).
- b) solo las actuaciones que alteran el correcto procesamiento de los datos contenidos en el sistema (tratamiento).
- c) solo aquellas actuaciones que dan lugar a un resultado del tratamiento objetivamente incorrecto (*output*).
- d) cualquier uso de sistemas informáticos que resulten idóneos para producir una transferencia no consentida de activos patrimoniales ajenos.

3. El consentimiento del titular de los activos patrimoniales transferidos mediante la comisión de un delito de estafa informática...

- a) determina siempre, y en todo caso, la atipicidad de la manipulación informática realizada.
- b) determina que la lesión producto de la transferencia de activos producida no pueda imputarse a la manipulación efectuada, lo que, sin embargo, no impide que se castigue a su autor por la tentativa de dicho delito.
- c) determinará a) o b) dependiendo de cuándo concurra su emisión.
- d) no tiene incidencia alguna, ya que lo que exige la estafa informática para ser apreciada es la ausencia del consentimiento del titular del sistema informático utilizado en su comisión.

4. Si un sujeto introduce unos datos falsos en un sistema informático de un banco para que el tratamiento automatizado y reiterado de los mismos lleve a que el sistema le transfiera cada mes, de forma automática y no consentida, una determinada cantidad de dinero de la entidad a su cuenta...

- a) comete un delito continuado de estafa informática.
- b) comete un delito de estafa informática que valorará y castigará el importe global de lo defraudado.
- c) comete tantos delitos de estafa informática como transferencias se hayan producido.
- d) Ninguna de las respuestas anteriores es correcta.

5. La utilización no autorizada de los datos de una tarjeta de crédito ajena para adquirir un producto en Internet, ocasionando con la compra el automático cargo de lo gastado en la cuenta corriente del legítimo titular de la tarjeta empleada...

- a) dará lugar al delito de estafa informática del artículo 248.2.a CP.
- b) constituye un delito de abuso de tarjeta de crédito del artículo 248.2.c CP.
- c) constituye a) o b) dependiendo de si la transferencia producida es revisada o no por un humano antes de ser efectuada.
- d) dará lugar a la apreciación del delito de estafa tradicional del artículo 248.1 CP.

6. Si un sujeto crea un programa que exclusivamente sirve para defraudar a todos los posibles cuentacorrentistas de una entidad bancaria y lo emplea, consiguiendo de esa forma que se le transfiera un importe total de 55.000 € de la cuenta de uno de ellos...

- a) cometerá el delito de estafa informática del tipo cualificado del artículo 250.1 CP.
- b) cometerá el delito de creación de programa informático específicamente destinado a cometer estafas del artículo 248.2.b CP.
- c) responderá de a) o de b) dependiendo de qué calificación tenga mayor pena.

d) responderá de un concurso de delitos entre a) y b).

Solucionario

Ejercicios de autoevaluación

1. c

2. d

3. c

4. b

5. b

6. d

Bibliografía

- Almela Vich, C.** (1998). «El delito de estafa y de apropiación indebida». *Actualidad Penal* (n.º 35).
- Faraldo Cabana, P.** (2009). *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*. Valencia: Tirant lo Blanch.
- Galán Muñoz, A.** (2004). «El nuevo delito del artículo 248.3 CP: ¿Un adelantamiento desmedido de las barreras de protección penal del patrimonio?». *Revista LA LEY* (n.º 6037).
- Galán Muñoz, A.** (2005). *La estafa y el fraude mediante sistemas informáticos. Análisis del artículo 248.2 CP*. Valencia: Tirant lo Blanch.
- Mata y Martín, R. M.** (2007). *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Cizur Menor: Aranzadi.
- Núñez Castaño, E.** (2017). *Manual de Derecho penal económico y de la empresa*. Valencia: Tirant lo Blanch.
- Quintero Olivares, G.** (2016). «De las defraudaciones». En: G. Quintero Olivares (dir.); F. Morales Prats (coord.). *Comentarios al Código penal español* (tomo II, 7.ª ed.). Cizur Menor: Aranzadi.
- Rovira del Canto, E.** (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.
- Sieber, U.** (1980). *Computerkriminalität und Strafrecht*. Colonia: Heyman.