Estudis de Dret i Ciència Política
Grau de Dret

El delito de estafa y los nuevos medios de pago

Sebastián Copman Spector

scopman@uoc.edu

enero de 2015

Actividad de Investigación

Trabajo Final de Grado

Curso 2015-2016 (2º semestre)

Índice

El delito de estafa y los nuevos medios de pago

Sebastián Copman Spector (scopman@uoc.edu)

Resumen

El presente trabajo pretende exponer las dificultades que plantea la introducción en España de nuevos medios de pago, en relación con la tipificación penal de las nuevas conductas ilícitas que estos permiten. El tipo básico de estafa, basado en el engaño del autor a la víctima, pronto se mostró insuficiente para abarcar los delitos cometidos por medio de tarjetas de crédito en terminales automáticos. La cuestión no se resolvió definitivamente con la tipificación de la estafa especial informática en términos excesivamente amplios, sino con la inclusión de un nuevo tipo más especifico, muchos años más tarde. Para entender y explicar la cabida de estos medios de pago en el marco jurídico español, se describe en primer lugar este marco y su evolución, para luego describir en qué consisten los nuevos medios de pago y cómo podrían tipificarse las conductas defraudatorias conocidas que puedan llevarse a cabo utilizándolos.

Palabras clave:
bitcoin, comercio electrónico, cartera electrónica, derecho, derecho penal, España, estafa, estafa informática, NFC, nuevos métodos de pago, pago contactless, pago con el móvil, tarjetas de crédito, teléfono móvil, TIC

Abstract

This paper aims to disclose the difficulties posed by the introduction of the new methods of payment in Spain, in order to qualify the new unlawful behaviours these systems allow according with the Spanish Criminal Code. The basic form of fraud, based on the deception of the victim by the perpetrator, soon proved insufficient to punish crimes committed via credit cards in automatic terminals. The issue was not finally resolved with the inclusion of the computer fraud as an offense in overly broad terms, but with the inclusion of a more specific offense, many years later. To understand and explain how these methods of payment fit in the Spanish law, this legal framework and its evolution are explained first, and then the paper describes the new methods of payment and some potential fraudulent behaviours that could be committed using them, aiming to qualify those behaviours according with the Criminal Code in force.

Keywords:
bitcoin, e-commerce, e-wallet, law, criminal law, Spain, fraud, computer fraud, NFC, new methods of payment, contactless payment, mobile payment, credit cards, mobile phone, IT

INTRODUCCIÓN

Justificación

Las nuevas tecnologías de la información y de la comunicación (TIC) se han convertido en una parte integrante y fundamental de nuestra sociedad, por lo que no resulta llamativo su relación con bienes jurídicos como el patrimonio individual, el orden socioeconómico o la seguridad en el tráfico jurídico. Los criminales han evolucionado al ritmo de las TIC, e incluso a veces han sido los protagonistas del desarrollo tecnológico; mientras que el derecho ha podido adaptarse de forma tardía e imperfecta, cuando lo ha hecho.

Las tarjetas de crédito tienen en España un uso generalizado desde principios de los años ochenta del siglo pasado, y su uso para la comisión de delitos está documentado por nuestros juristas al menos desde 1989. A pesar de ello, entre los penalistas españoles son conocidas las dificultades para tipificar conductas lesivas realizadas por medio de tarjetas de crédito sobre los bienes jurídicos mencionados y el intenso debate doctrinal existente entonces al respecto, hasta la reforma operada por la Ley Orgánica (LO) 5/2010, de 22 de junio, en el Código Penal (CP). Y esta tecnología no es precisamente la más nueva o la que más ha evolucionado.

Es inminente la llegada a España de los sistemas de pago a través del teléfono móvil, instrumento ubicuo y esencial en nuestra sociedad; mientras la utilización de nuevos sistemas como las criptodivisas, que no son sólo medios de pago sino bienes inmateriales en sí mismos, comienza a ser más que incipiente. Sobre estos instrumentos aún no se ha pronunciado el legislador penal, y la jurisprudencia y la doctrina son casi inexistentes; por lo que parece inevitable que vuelvan a presentarse las dificultades y los debates a los que se hizo referencia.

Objetivo y alcance

Este trabajo se centrará en estos ataques en relación al patrimonio individual de las víctimas, con especial atención al delito de estafa y su tipificación en España. A diferencia de lo manifestado sobre el repertorio jurídico, la información técnica sobre estos nuevos medios de pago es profusa, por lo que es posible analizar su cabida en el marco jurídico vigente. A su vez, la documentación práctica y la exposición teórica de conductas injustas utilizando estas modalidades en otros ordenamientos hacen posible el ejercicio de encajar estos comportamientos al Código Penal español. En primer lugar se procurará explicar la adaptación de este tipo penal para abarcar las nuevas conductas ilícitas que permitían las tarjetas de crédito o débito, y el tratamiento que se daba a estas defraudaciones antes de las reformas en el tipo. En el segundo apartado, se explicará el funcionamiento de los nuevos medios de pago analizados. La elección del *bitcoin* como caso de estudio se debe principalmente a que esta criptomoneda es la más conocida y cotizada, y a que el resto de criptodivisas se basan en su protocolo. Con estas premisas, se intentará encajar las posibles conductas injustas sobre estos medios de pago a las distintas modalidades de estafa contempladas en el CP. Los problemas que se encuentren en el camino, y las importantes implicaciones que estos nuevos medios de pago puedan tener en otros aspectos, por su alcance global o su afectación sobre otros bienes jurídicos, se expresarán en el cuarto apartado.

1 EL DELITO DE ESTAFA Y SU EVOLUCIÓN

La definición del delito de estafa por parte del legislador penal se lleva a cabo con la LO 8/1983, de 25 de junio, de reforma urgente y parcial del Código Penal, refundido entonces, conforme a la Ley 44/1971, de 15 de noviembre, en el Decreto 3096/1973, de 14 de setiembre (CP1973). Hasta ese momento, tal como manifiesta la Exposición de Motivos de la reforma, la formulación de la estafa dependía en exceso del análisis casuístico en los tribunales, que algunas veces encontraban serias dificultades para castigar estos ataques contra el patrimonio, pero que con mayor asiduidad aplicaban castigos excesivos atendiendo al sistema de cuantías vigente entonces.

Con la evolución tecnológica los ataques al patrimonio se han desarrollado de formas que difícilmente podrían tener cabida en esa definición, por lo que la intervención del legislador ha tenido que ser reiterada para respetar los principios de seguridad jurídica y legalidad penal.

1.1 El tipo básico de estafa

La LO 8/1983 dejó el art. 528.I CP1973 redactado de la siguiente forma:

> *"Cometen estafas los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de tercero"*

Esta formulación del concepto básico de estafa se ha mantenido con la promulgación del nuevo Código Penal de la LO 10/1995, cuyo art. 248.1, inalterado desde entonces, establece que:

> *"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"*

Por tanto, son elementos esenciales del concepto básico de estafa: un engaño idóneo, el error de la víctima, un acto de disposición patrimonial y un perjuicio económico; a lo que hay que sumar las exigencias del tipo subjetivo: el dolo específico de producir el engaño y el ánimo de lucro. Además, como en toda conducta que se intente calificar como antijurídica, deben cumplirse los requisitos para atribuirle relevancia típica y establecerse la relación de causalidad entre la misma y la imputación objetiva del resultado.

La discusión suele girar en torno a la idoneidad del engaño producido por el autor en la víctima. En principio, si el error se ha producido es porque el engaño ha sido idóneo para ello, aunque también puede rechazarse la suficiencia del engaño cuando no habría sido verosímil para ninguna persona en su sano juicio. Del mismo modo, se suele apreciar una ruptura en el nexo causal cuando la víctima podría haber evitado el error llevando a cabo las comprobaciones más elementales, en cuyo caso el acto de disposición será producto de una negligencia. Estas circunstancias pueden considerarse bien en abstracto o bien de acuerdo con las capacidades concretas de la víctima. El acto de disposición por parte de la víctima puede ser activo u omisivo, y ser la causa del desplazamiento patrimonial que provoca el perjuicio.

1.2 La estafa de manipulación informática

La introducción de la informática en la gestión y asignación de activos patrimoniales ha permitido que, haciendo uso de estos sistemas, se puedan realizar transmisiones injustas de

dichos activos. Sin embargo, estos casos no podían reconducirse al delito de estafa, ya que la víctima no sufría un engaño ni realizaba un acto de disposición. Así mismo, parte de la doctrina afirmaba que la interacción del perpetrador se realizaba con un equipo que no podía ser engañado. Hasta su configuración legal específica los tribunales sólo podían castigar estos casos, cuando el perpetrador podía considerarse apoderado de los activos desviados, subsumiendo la conducta en el tipo penal de la apropiación indebida del art. 535 CP1973, como se refleja en la sentencia del Tribunal Supremo (STS, SSTS) de 19 de abril de 1991 (*v.* Anexo I). No fue hasta la aprobación del Código Penal de 1995 que se tipificó esta conducta en su artículo 248.2 como una estafa especial:

> *"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."*

Pero esta previsión tampoco supuso una solución definitiva. Parte de la doctrina consideraba aplicable el entonces vigente art. 248.2 CP cuando la transferencia no consentida se realizaba sólo por medios informáticos manipulados o afectados por algún artificio; debiendo subsumir las conductas delictivas en el tipo básico cuando, a pesar de la manipulación informática, el destinatario del engaño y quien sufre el error es un ser humano. La postura contraria consideró más amplia la aplicación del nuevo tipo, por lo que entendía subsumible en el mismo prácticamente cualquier enriquecimiento injusto derivado de un uso normal de cualquier equipo informático no manipulado, de manera artificiosa.

Posteriormente, la LO 15/2003 introdujo un tercer apartado al art. 248 CP que tipificó la fabricación, introducción, posesión o facilitación de programas informáticos para la comisión de estafas. Su objeto son los programas destinados específicamente y objetivamente aptos para la comisión de cualquier tipo de estafa. Es decir, el programa capaz de producir un perjuicio en las manos de un usuario experto, pero no cuando es utilizado por un usuario común o medio, no sería objeto de este tipo penal.

1.3 La estafa mediante tarjetas de crédito o débito, o cheques de viaje

Con la aprobación de la LO 5/2010, de 22 de junio, se suprime el art. 248.3 CP y el art. 248.2 CP queda redactado, hasta día de hoy, en los siguientes términos:

> *"También se consideran reos de estafa:*
>
> *a) Los que, 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.*
>
> *b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.*
>
> *c) 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."*

Así, a los supuestos de estafa existentes se sumaba uno específico para la utilización de medios de pago distintos al dinero. Ahora bien, esto no quiere decir que con anterioridad no se castigasen delitos cometidos utilizando dichos medios. Su uso para la extracción de dinero en efectivo de cajeros automáticos, al principio se subsumía en el tipo de robo con fuerza en las cosas, doctrina apoyada por la SSTS 257/2000, de 18 de febrero (rec. 504/1998, *v.* Anexo II). Como ya se mencionó, la utilización de tarjetas de crédito o de débito sólo para compras en establecimientos comerciales podían calificarse tanto como estafas del tipo básico como

estafas informáticas; y en ambos casos era común que se aprecie un concurso medial con un delito de falsedad, por el hecho de firmar cupones. Si el autor utilizaba una tarjeta auténtica para retirar dinero en efectivo de cajeros y para realizar compras, se le castigaba como autor del delito de robo con fuerza en las cosas y como autor del delito de estafa, este último en concurso medial con un delito de falsedad, como se puede ver en la STS 2016/2000, de 26 de diciembre (rec. 254/1999, *v.* Anexo III). Tanto la calificación de la extracción de dinero de cajeros como robo con fuerza en las cosas, como la exasperación punitiva con la que se resolvían casos como el último fueron objeto de censura desde el primer momento. Posteriormente, tanto los casos de extracción de dinero en efectivo como los de compras en establecimientos con tarjetas ajenas y auténticas pasaron a considerarse por el Tribunal Supremo como estafas informáticas del art. 248.2 CP, con lo que ya no se podían dar concursos reales en casos como el anterior, tal como manifiesta el Alto Tribunal en su STS 369/2007, de 9 de mayo (rec. 11142/2006, *v*. Anexo IV).

La reforma operada por la LO 5/2010 resolvió de forma definitiva la cuestión, ya todo el desvalor de la acción consistente en lograr transferencias patrimoniales injustas utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos contenidos en tales medios de pago auténticos, queda contemplado en el nuevo art. 248.2.c) CP. Así mismo, dicha reforma también solucionó los problemas relativos a la consideración de las tarjetas bancarias como moneda, en sede de falsedades, con la modificación del art. 387 CP y la introducción del art. 399 bis CP. Aunque los ataques contra la seguridad en el tráfico jurídico, el bien jurídico protegido con la tipificación de las falsedades, no son objeto de este trabajo, es importante señalar la coherencia sistémica y la adecuación material que alcanza la tutela penal relativa a los medios de pago con las novedades introducidas por la LO 5/2010.

2 LOS NUEVOS MEDIOS DE PAGO

Desde hace unos años se ha ido extendiendo la utilización de nuevos medios de pago no contemplados expresamente por el legislador español. Algunos llevan mucho tiempo siendo utilizados de forma generalizada en España, como las carteras electrónicas tipo *PayPal*, mientras otros como el *bitcoin* son casi desconocidos. Por otro lado, las principales empresas que ofrecen el servicio de pago con el teléfono móvil anuncian su entrada en el mercado español a principios de 2016.

2.1 El pago con dispositivos móviles

Bajo esta definición en sentido amplio se engloban los servicios de pago operados bajo regulación financiera que se lleven a cabo a través de un dispositivo móvil. En lugar de utilizar efectivo o tarjetas de crédito, el usuario realiza el pago con el teléfono móvil para comprar bienes o contratar servicios.

Ahora bien, aunque el instrumento concreto con el que se realiza la acción del pago sea siempre el mismo, para el objeto de este estudio es importante distinguir la cuenta en la que se produce el cargo. Con los pagos fraudulentos que estén asociados directamente a tarjetas de crédito o débito auténticas o a los datos obrantes en ellas no habría problemas para calificarlos como estafas del actual art. 248.2.c) CP, independientemente de la modalidad concreta: en web, con una aplicación, confirmando el pago con tarjeta con código enviado por SMS, sistemas de pago específicos de fabricantes (como *Apple Pay, Samsung Pay,* etc.), siempre que lleven asociados tarjetas de crédito o débito, etc.. Del mismo modo, los pagos asociados a carteras electrónicas tendrán el tratamiento legal que se dé a los mismos (*v. infra*, 2.2).

Para todos los sistemas mencionados es necesario que quien pretende realizar el pago se dé de alta y contrate otro servicio: abrir cuenta bancaria, solicitar una tarjeta de crédito y/o abrir una cartera electrónica. Sin embargo, existen sistemas que no precisan estos pasos previos, como la facturación directa asociada al número de móvil, que se basa en que los clientes ya tienen, bien una relación contractual con el operador de telefonía, o bien un crédito asociado a su número. Los cargos se reflejan en la siguiente factura del usuario de contrato, o se debitan del saldo del usuario de prepago, y no están asociados a ninguna tarjeta de crédito o cuenta bancaria.

Otros sistemas asociados al fabricante del dispositivo (*Apple, Samsung,* etc.) se basan en la tecnología de comunicación de campo cercano (*near field communication* en inglés, o NFC) y la encriptación de datos de manera local, en el mismo aparato. En principio y hasta hoy, la información almacenada y utilizada por estos sistemas son relativas a tarjetas de crédito o carteras electrónicas, pero ya se están desarrollando herramientas de pago que utilizan esta tecnología NFC de los teléfonos móviles más modernos sin necesidad de vinculación con tarjetas de crédito o carteras electrónicas conocidas. Algunos de estos sistemas ya incorporan como segundo factor de autenticación las huellas dactilares del usuario. La utilización de datos biométricos como acceso seguro es siempre objeto de un intenso debate que compara sus riesgos con sus beneficios. Sin entrar ahora en consideraciones acerca del derecho a la intimidad o al derecho de control que los ciudadanos pueden ejercer sobre sus datos personales, una huella digital parece una forma más segura y menos falible que una contraseña, para permitir el acceso que sea solo a la persona que debería tener dicho acceso; pero un PIN o una contraseña comprometidos pueden cambiarse muy fácilmente, en la mayoría de los casos.

La tecnología NFC es la misma utilizada en las tarjetas *contactless*, por lo que las limitaciones técnicas que impiden que el pago *contactless* con el móvil sea generalizado en España se podrían solucionar con actualizaciones de *software* relativamente sencillas y económicas. Si estos sistemas no están disponibles aún en España, en algún momento fue por la falta de interés de las compañías prestadoras, dada la escasa implantación en nuestro mercado de los modelos con chip NFC; y ahora es por la falta de acuerdo acerca de las comisiones, entre estas empresas y las principales entidades emisoras de las tarjetas asociadas.

2.2 Carteras electrónicas

Las carteras electrónicas (o virtuales) son servicios en línea que permiten a los usuarios controlar y almacenar en un solo lugar toda la información necesaria para comprar, como nombres de usuario y contraseñas, dirección de envío, información de tarjetas de crédito o cuentas bancarias, etc.

En sus orígenes su uso sólo se concebía en el comercio electrónico, pero ahora empieza a ser frecuente su uso para pagos presenciales en establecimientos comerciales aprovechando la tecnología NFC o la lectura óptica de códigos QR, ya sea por medio de dispositivos móviles o mediante carteras electrónicas específicas de hardware: unos llaveros con chip NFC y/o pantalla para mostrar códigos QR, que almacena las claves para acceder al servicio de cartera electrónica. Aunque conceptualmente pueda parecer que estas carteras son sólo un almacén de información de otros medios de pago, en realidad las carteras electrónicas tienen fondos propios, que no tienen por qué depender de aquellos medios. El usuario básico normalmente tendrá su saldo en cero, al realizar la compra seleccionará una tarjeta, se hará el cargo por el importe necesario en la tarjeta para el traspaso de los fondos a la cartera, que es de donde se realiza el pago, resultando normalmente un saldo en cero. Pero muchos usuarios realizan traspasos a sus carteras para mantener saldos positivos, en algunos casos para aprovechar ofertas o promociones; y otros muchos usuarios utilizan estas carteras para recibir cobros. Es decir, es posible contar con fondos en muchos de estos servicios sin asociar ninguna tarjeta de crédito o cuenta bancaria.

2.3 El bitcoin

Una divisa o moneda virtual es una clase de dinero digital desregulado, la cual es aceptada y utilizada entre los miembros de una comunidad virtual específica. Entre ellas están las divisas virtuales estancas, que son adquiridas por los usuarios al desarrollador por medio de una suscripción fija, para luego ser utilizadas en el mercado de la comunidad, sin que haya flujo de divisas virtuales con el exterior de la comunidad (como el oro del juego de rol en línea *World of Warcraft*). También están las divisas virtuales de flujo unidireccional, que los usuarios pueden adquirir directamente del desarrollador con divisas reales a una tasa de cambio o tarifa determinada, pero que luego no son convertibles a dinero real. Por último, existen divisas virtuales de flujo bidireccional, que pueden tanto ser compradas con dinero real, como vendidas por dinero real (por ejemplo, los dólares Linden de *Second Life*). El bitcoin se encuentra dentro de esta última clase, pero lo que la hace particular es haber sido la primera y ser la más importante criptodivisa descentralizada.

2.3.1 Origen e historia

Ya en la última década del siglo pasado circulaban artículos sobre sistemas descentralizados y anónimos de transferencia de dinero, de usuario a usuario (*peer-to-peer,* P2P), pero ninguno de ellos ha sido viable. Pero en octubre de 2008 Satoshi Nakamoto (se cree que es un seudónimo de un grupo de personas) publica su artículo *Bitcoin: A peer-to-peer electronic cash system* en una lista de correo sobre criptografía*,* y en enero de 2009 lanza la primera versión del software bitcoin como código abierto y emite los primeros bitcoins, que al principio no tenían ningún valor. Estas unidades monetarias, que son divisibles hasta en 8 dígitos, tuvieron su primera tasa de cambio con el dólar cuando en octubre de ese año una ecuación calculó el coste de electricidad para su generación: 1 dólar = 1.309,03 bitcoins (BTC). Lo que comenzó como un experimento o juego entre fanáticos de la criptografía y la economía que se enviaban cantidades de una divisa de valor testimonial, durante 2010 comenzó a incorporar transacciones con dinero real. Al principio de manera privada entre los usuarios del foro y del canal de chat, pero antes de finales de año ya se abrían los primeros *exchanges*, webs especializadas que operan como casa de cambio entre bitcoins y otras divisas, de las que hay cientos hoy en día. De este modo, el valor del bitcoin fluctúa según la oferta y la demanda, y alcanza la paridad con el dólar en febrero de 2011. A 1 de enero de 2016 la unidad de bitcoin (BTC), de las que se han emitido unos 15 millones, se cambia en torno a los 400€, lo que hace una capitalización cercana a los 6.000 millones de euros. Y esto solo en bitcoins, ya que existen aproximadamente unas 600 criptodivisas similares, aunque con una importancia bastante inferior. Estos valores deben verificarse constantemente ya que el mercado de las criptodivisas se caracteriza por su volatilidad.

2.3.2 Concepto

La piedra angular del sistema del bitcoin es una base de datos abierta y distribuida denominada cadena de bloques o *blockchain*, que es el libro de registro de todas las transacciones verificadas y de todas las unidades de la divisa emitidas. En vez de confiar esta contabilidad a una autoridad central, el mantenimiento del registro lo lleva acabo una red P2P de ordenadores que ejecutan el software bitcoin. Este protocolo contiene de manera predefinida las condiciones para la emisión de nuevos bitcoins y su atribución (así como su límite absoluto, marcado en 21.000.000 de bitcoins), y la llave pública que permite la verificación de las transacciones firmadas por los usuarios con sus respectivas llaves privadas. Así, los nodos de la red van validando las transacciones, agregándolas en su copia del registro, y transmitiendo sus enmiendas al registro a los otros nodos que ejecutan el programa. La plenitud,

consistencia e inalterabilidad de los registros depende de los mineros (*miners,* en inglés), que son los usuarios que aportan a la red su mayor capacidad de procesamiento, por lo que reciben bitcoins. Esta tarea se denomina minería porque con la resolución de complejas operaciones matemáticas se lleva a cabo la comprobación del registro y se van añadiendo nuevos bloques válidos al mismo, generándose (emitiéndose) nuevos bitcoins aproximadamente cada 10 minutos. Los mineros también pueden recibir como compensación una pequeña parte de las transacciones que verifican, a modo de tasa de transferencia. El protocolo bitcoin también contiene las condiciones para que la dificultad de los problemas matemáticos a resolver aumente a medida que mejora el desempeño de las tareas de minería. De esta manera el flujo de bitcoins se ajusta al desarrollo de la capacidad de procesamiento de la red en su conjunto (control de inflación); al mismo tiempo que, cuanto mayor sea el poder de procesamiento individual, mayores posibilidades habrá de obtener bitcoins por medio de la minería (mayor recompensa a los individuos que más aportan a la comunidad).

La titularidad de los bitcoins está íntimamente relacionada con la llave privada que permite firmar digitalmente las transacciones que salgan de una dirección específica. Sin la clave privada no se pueden firmar transacciones y los bitcoins no se pueden transferir ni gastar de ningún modo. Como no hay autoridad que controle la divisa, es imposible recuperar estas claves, al igual que deshacer transacciones o practicar cualquier embargo o cobro coercitivo sobre los bitcoins de quien conserve segura su clave privada.

Por estas características suele ser comparado con el dinero fiduciario (esto es, las divisas reales, que dependen de la confianza de la comunidad y no están respaldadas por nada que no sea una promesa de pago del emisor, una entidad centralizada y monopolística) y con valores como el oro: es escaso, o difícil de crear o encontrar; es durable, es transportable, es divisible, aunque es difícil de falsificar su autenticidad es verificable, puede ser almacenado y es fungible.

2.3.3 Tratamiento jurídico en España

La calificación del bitcoin por parte de las autoridades españolas sólo se encuentra en respuesta de consultas de sus ciudadanos sobre cuestiones fiscales y contables. Se pueden examinar las consultas vinculantes V2228-13 y V1028-15 relativas a la apertura de servicios de *exchange* en España, dictadas por la Dirección General de Tributos, en las que se aclara la relevancia del bitcoin en los estados contables para la tributación del Impuesto de Sociedades, si las operaciones de compra o venta de bitcoins están sujetas o no a tributación por el Impuesto sobre el Valor Añadido (IVA), y cuando están sujetas, si están amparadas por alguna exención.

Esta doctrina administrativa ha quedado desplazada por la sentencia del Tribunal de Justicia de la Unión Europea (TJUE), Sala 5ª, Asunto C-264/14, de 22 de octubre de 2014 (Skatteverket / David Hedqvist). En ella se responde la cuestión prejudicial planteada por un tribunal de Suecia, que debía resolver sobre la tributación por IVA de un servicio de cambio de divisas con bitcoins abierto allí. Entendido el servicio como oneroso, en tanto las operaciones de su titular se encaminan a obtener una ganancia resultante de la diferencia entre el precio por el que vende las divisas y el precio que está dispuesto a pagar, el TJUE interpreta que estas operaciones están sujetas a IVA, de acuerdo con el art. 2.1.c) de la Directiva 2006/112/CE del Consejo, de 28 de noviembre. Pero del mismo modo, entiende que en estas transacciones el bitcoin tiene la finalidad exclusiva de ser un medio de pago, por lo que debe interpretarse que están amparadas por la exención prevista en el art. 135.1.e) de la Directiva 2006/112/CE. Es decir, de acuerdo con el TJUE el intercambio de bitcoins por divisas tradicionales está sujeto al IVA pero exento de tributar por el impuesto, como ocurre cuando el intercambio es entre distintas divisas tradicionales.

Aparte de esto y alguna declaración en informes de órganos políticos supranacionales, no existe ninguna definición del bitcoin con valor jurídico aplicable a España, aunque este problema se da en la casi todos los países.

3 ATAQUES UTILIZANDO LOS NUEVOS MEDIOS DE PAGO: SU TIPICIDAD COMO ESTAFA

Este apartado pretende describir las conductas injustas que pueden llevarse a cabo utilizando los nuevos medios de pago descritos, y analizar su posible relevancia penal de acuerdo con la legalidad vigente, con especial atención al delito de estafa. Algunos de estos ataques ya han sido documentados en la práctica (aunque sólo unos pocos en España) y otros son meras formulaciones teóricas cuyas probabilidades de ejecución satisfactoria son muy bajas en el estado actual del desarrollo tecnológico, pero que no deberían descartarse como consideración de futuro. Justamente por dicha razón, en ningún caso debe considerarse esta lista como exhaustiva.

3.1 Dispositivos móviles y carteras electrónicas

Las vulnerabilidades de los modernos dispositivos móviles son varias. Como cualquier ordenador portátil, se conecta a internet en una pluralidad de redes inalámbricas de fiabilidad dudosa; y aun conectado a una red fiable, pueden ser aprovechadas las vulnerabilidades en su navegador, en las aplicaciones que ejecute y en su propio sistema operativo. Esto sin tener en cuenta las modificaciones que hacen a veces los propios usuarios en estos elementos, a través de la técnica de *rooting* o *jailbraking*.

Por otro lado, los dispositivos con tecnología NFC podrían conectarse a otros aparatos cercanos sin requerir ninguna acción por parte del usuario. Esto ya ocurre con las tarjetas *contactless*: alguien podría acercar a bolsos y bolsillos un TPV inalámbrico con un cargo preparado de un máximo de 20 €, hasta lograr la aceptación de alguna tarjeta con NFC; y es por esta razón que se establece aquel tope en estas transacciones. Pero los dispositivos móviles permiten una interacción más compleja por este mismo protocolo, que no es único ni es seguro en sí, sino que los desarrolladores han eliminado las posibles vulnerabilidades a distintos niveles de software, bajo varios estándares en un mercado muy segmentado. Fruto de ello es la mencionada evolución a sistemas NFC de doble factor de autenticación, como *Apple Pay* o *Samsung Pay*, de inminente llegada a España y que por su mayor seguridad permitirán pagos sin más límite que el de nuestra cuenta.

En principio, no habría problema en entender cualquiera de estos ataques como una manipulación informática, con lo que estarían tipificados en el art. 248.2.a) CP. La cuestión es que el tipo de estafa por medio de tarjeta de crédito o de débito, o de cheques de viaje, del art. 248.2.c) CP es de aplicación preferente de acuerdo con el principio de especialidad (art. 8.1ª CP). En definitiva una correcta descripción de la conducta típica, con la redacción actual del art. 248 CP, depende más de la cuenta en la que se realice el cargo de los pagos fraudulentos que del ataque realizado o la vulnerabilidad aprovechada.

De acuerdo con la encuesta y el estudio presentados por la Reserva Federal de los EE.UU. en marzo de 2015 (*v.* Anexo V), de las personas que hacen pagos con dispositivos móviles, un 55% hace cargos en sus tarjetas de débito, un 51,2% hace cargos en tarjetas de crédito, un 40,7% directamente en cuentas bancarias (sin tarjetas de crédito o débito), un 15,4% en cuentas no bancarias como las carteras electrónicas, un 7,6% utiliza tarjetas de débito prepagas y un 4,2% transfiere cargos a su factura telefónica. De estos datos se puede inferir

que la mayoría de las transferencias fraudulentas por medio del móvil se deberían enjuiciar según el art. 248.2.c) CP.

Lo mismo ocurre con las operaciones ilícitas realizadas con carteras electrónicas, tanto si se hubiera accedido a estas directamente o a través de un dispositivo móvil, siempre que en las operaciones se utilicen los datos de tarjetas de crédito o débito auténticas.
El resto de operaciones deberá reconducirse al tipo de estafa informática del art. 248.2.a) CP, independientemente de que la cuenta de cargo sea bancaria, de fondos independientes en carteras electrónicas o cualquier otro sistema, aprovechando la antes mencionada doctrina del Tribunal Supremo, que interpreta este precepto de forma amplia. Puede apreciarse la manipulación informática, su autor consigue la transferencia no consentida de un activo patrimonial y perjudica a tercero. La aplicación de las defraudaciones del fluido eléctrico y análogas, y de uso no autorizado de equipo de telecomunicaciones, de los arts. 255 y 256 CP, debe descartarse. Tanto el tipo de estafa informática como el de estafa por medio de tarjetas serían de aplicación preferente por consunción, ya que ambos describen mejor el desvalor de la acción en sus respectivos casos.

Pero no olvidemos que los dispositivos móviles pueden perderse o hurtarse con relativa facilidad. Si un nuevo poseedor no hace ninguna manipulación informática, y realiza cargos que perjudiquen a otro, sin datos asociados a ninguna tarjeta de crédito o débito ¿En estos casos, podrían renovarse discusiones doctrinales superadas como ocurría con las tarjetas de crédito antes de la reforma operada por la LO 5/2010? La lógica indica que no, porque antes de la entrada en vigor de la reforma, la doctrina del Tribunal Supremo que entendía la tipificación de cualquier transferencia ilegítima realizada con tarjetas de crédito en un terminal automático como estafa informática era de aplicación pacífica y mayoritaria (*v.* STS 369/2007, de 9 de mayo, Anexo IV). Es decir, no hace falta que la manipulación informática sea artificiosa, sino que para la realización del tipo basta una manipulación normal.

3.2 Bitcoin

La seguridad de los bitcoins puede analizarse en dos niveles. Como sistema, las características de la *blockchain* y de la red P2P hacen prácticamente imposibles las modificaciones de la historia de transacciones, que se van confirmando casi instantáneamente. Sólo en el caso hipotético de que un individuo aportase más de la mitad de la capacidad de procesamiento de toda la red, éste podría evitar la confirmación de nuevas transacciones, revertir las últimas de cualquier usuario, o realizar doble gasto de sus bitcoins. Pero no podría alterar el registro histórico, ni crear nuevas unidades de bitcoin, más allá de las que consiga por minería; ni transferir los bitcoins de otros usuarios, por no contar con las claves privadas. Estos ataques afectarían el patrimonio de los usuarios en tanto con su éxito se produzca una depreciación de la moneda virtual, en cuyo caso corresponderá enjuiciar los hechos de acuerdo con tipos penales que protejan bienes jurídicos supraindividuales.

A nivel de usuario, todo se reduce a la clave privada con la que puede firmar digitalmente las transacciones desde su dirección. Por la fortaleza de este sistema también es muy difícil embargar o ejecutar bitcoins, y hay bitcoins con claves privadas perdidas u olvidadas que permanecerán bloqueados de manera perpetua.

Por tanto, es normal que todos los casos conocidos de sustracción de bitcoins u otras criptomonedas tengan su origen en el acceso a la clave privada. La particularidad de estos ataques es que no se suelen dirigir contra usuarios individuales, sino contra empresas que tienen confiadas las claves privadas de aquellos. Por ejemplo, carteras electrónicas que manejen bitcoins, llaveros electrónicos y administradores de contraseñas, o cualquier servicio de *exchange* que acepte depósitos en bitcoins. También es común que los usuarios, del mismo modo que llevan una pequeña parte de su dinero en la cartera y guardan sus ahorros en otro lugar u otros lugares; utilicen varios monederos bitcoin, cada uno con su dirección, para el

manejo de distintas cantidades de moneda y apliquen distintas medidas de seguridad en cada uno de ellos.

Siguiendo con lo afirmado en el subapartado anterior, teniendo en cuenta las características del sistema, la equiparación del bitcoin al resto de divisas por parte del TJUE (al menos respecto a la tributación por IVA de su compra o venta) y la última doctrina pacífica del Tribunal Supremo relativa los gastos fraudulentos por medios de pago no expresamente tipificados, cualquier transferencia no consentidas de bitcoins debería subsumirse en el tipo de estafa informática del art. 248.2.a) CP..

Además, como ocurre con cualquier otro activo patrimonial, el bitcoin puede ser objeto del tipo básico de estafa, cuando la transferencia no tiene su origen en una manipulación informática sino en un acto de disposición del perjudicado, producto de un engaño idóneo. Como ejemplo sirven los esquemas piramidales desmontados en EE.UU. por la *Securities and Exchange Commission* (SEC), por los que los autores pedían a las víctimas que inviertan sus bitcoins y capten nuevos inversores. El capital recaudado se destinaría supuestamente a una operación de minería masiva que arrojaría pingües beneficios para repartir entre los inversores, cuando en realidad es apropiado por los creadores del plan.

El problema, dadas las posibilidades de anonimato que ofrece el bitcoin que hacen casi imposible conocer el autor de las transacciones, es que muchos casos pueden parecer estafas informáticas masivas, con un depositario de fondos o claves privadas de terceros alegando que su clave privada ha sido hackeada; cuando en realidad el depositario es el autor de la estafa.

Para acabar, por el aumento del número de usuarios que minan y el desarrollo de los procesadores, cada vez es más difícil resolver los problemas matemáticos planteados por el protocolo bitcoin, y los costes de inversión y de energía eléctrica necesarios para minar nuevos bitcoins tiende a equipararse con el valor de los nuevos bitcoins que pueden obtenerse mediante minería. Ante esta situación, algunos *hackers* han desarrollado programas maliciosos que subrepticiamente toman el control de otros ordenadores para que aporten poder de procesamiento a la actividad de minería de quien despliega el *malware*. Aunque un ordenador personal común poco podrá aportar en una operación de minería, estos ataques pueden llegar a infectar decenas de miles de ordenadores, lo que mantiene un cierto incentivo para su perpetración. Ahora bien, el beneficio en bitcoins del autor no es correlativo con el perjuicio que sufre la víctima, que si fuera usuaria de esta moneda no vería sus fondos comprometidos por este ataque. El perjudicado verá incrementado su consumo eléctrico y puede llegar a notar que su ordenador "va lento", por lo que estas conductas sólo podrían considerarse defraudatorias en relación al fluido eléctrico (art. 255 CP), aunque evidentemente también podrían enjuiciarse como daños informáticos (arts. 264; 264 bis; 264 ter y 264 quater).

4 IMPLICACIONES ÉTICAS Y SOCIALES

La garantía criminal contenida en el principio de legalidad penal (art. 1.1 CP y art. 25.1 de la Constitución Española) exige que las prohibiciones se establezcan de manera clara y de la forma más precisa posible, debiéndose evitar los términos demasiado amplios, vagos o confusos. No se debe olvidar que ya estando tipificado el delito de estafa informática, la extracción de dinero en cajeros automáticos con tarjetas de crédito o débito se siguió castigando como robo con fuerza en las cosas durante varios años. Para encajar las conductas injustas que permiten los nuevos medios de pago en la redacción actual del tipo especial de estafa informática se depende de una doctrina establecida por el Tribunal Supremo en 2007, justamente ampliando el ámbito de aplicación del término "manipulación", que ya es bastante vago de por sí.

Los teléfonos y otros dispositivos móviles no es que sean de uso generalizado, sino que ya se los puede calificar como ubicuos; con la especial particularidad de que muchos de sus usuarios son menores de edad. A esto hay que sumar el desarrollo de la llamada internet de las cosas, que está trayendo nuevos aparatos conectados a la red que pueden realizar pagos, incluso automáticamente, sin necesariamente ser móviles (como las neveras que hacen la compra para reponer lo agotado). El uso de estos dispositivos es todavía incipiente, pero nada nos impide imaginar que el mismo sea bastante más extendido en un futuro próximo.

Por otro lado, la necesaria conexión a internet para la utilización de estos nuevos medios de pago rompe toda frontera para los posibles autores de estos delitos, con las dificultades que ello trae a la hora de determinar el lugar de su comisión y el alcance de la jurisdicción española para juzgarlos (art. 23.1 LO del Poder Judicial).

En el caso concreto de las criptomonedas descentralizadas, sus características hacen prácticamente imposible averiguar la autoría real de las transacciones de los usuarios que quieren ocultarse. Si bien su cambio por otra divisa suele estar sujeto a las mismas exigencias que otras operaciones financieras de acuerdo con la legislación antiblanqueo (en España, Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo), muchos servicios de *exchange* se ubican en territorios sin normas de este tipo, o de cumplimiento ni siquiera testimonial, donde los fondos de origen fraudulento pierden su rastro. El uso de estos nuevos activos patrimoniales es incipiente, pero crece de manera exponencial. Muchos analistas sostienen que no es más que otra burbuja sobre un activo, pero otros expertos sostienen que las criptodivisas son el futuro, lo cual tiene verdadero potencial disruptivo.

CONCLUSIONES

La ajustada sanción penal a los ataques fraudulentos contra el patrimonio a los que da acceso el desarrollo tecnológico, requiere una adaptación de los tipos penales para que contemplen estas conductas. Mientras eso no ocurre, los criterios jurisprudenciales pueden ser divergentes, y la doctrina del Tribunal Supremo, cambiante; lo cual afecta a la seguridad jurídica.

Mientras la inmensa mayoría de las transacciones fraudulentas pueda reconducirse a cargos en tarjetas de crédito o débito (y todo indica que esta será la situación, al menos en el medio plazo), la tutela penal sobre las operaciones con nuevos medios de pago será adecuada. Pero cuando esto ya no sea así, del mismo modo que el legislador penal ha debido introducir el tipo específico de estafa mediante estas tarjetas, por lo generalizado de su uso fraudulento, quizás sea el momento de modificar el art. 248.2 CP.

Debe encontrarse el equilibrio entre las exigencias del principio de legalidad y los usos sociales resultantes del desarrollo tecnológico, lo que requerirá la constante intervención del legislador penal. Otra solución podría ser la técnica legislativa de la norma penal en blanco, por la que el precepto penal describe el núcleo de la conducta prohibida y deja los aspectos adyacentes o secundarios a lo regulado en disposiciones de distinto orden o de rango inferior, a las cuales remite de manera clara.

Por su carácter descentralizado, las criptomonedas no tienen fronteras, no pueden modificarse ni adaptarse a normativa alguna, ni tienen una autoridad a la que se le pueda requerir una conducta determinada. Aunque los valores de capitalización de sus mercados sea elevado, su uso no deja de ser incipiente, al menos en el tráfico legítimo. La respuesta normativa a la criptografía, tanto a nivel nacional como internacional, difícilmente será ejecutable.

VALORACIÓN

Si bien la metodología de estudio de la *Universitat Oberta de Catalunya* requiere y promueve el uso y el aprendizaje de competencias investigadoras a lo largo de todos los estudios del Grado de Derecho, este trabajo ha significado una evolución. El dossier de investigación ha obligado a la toma de una postura activa para escoger su temática y los aspectos específicos de la misma a desarrollar.

La definición del tema ha necesitado un trabajo de investigación previo. Muchas eran las hipótesis que se podían plantear y las dudas que se podían investigar, en relación a las notas informativas trabajadas durante el presente curso. Algunas de estas hipótesis parecían llevar a investigaciones eternas e infructuosas, mientras otras se consideraron demasiado superficiales e inadecuadas para llevar a cabo una investigación mínimamente profunda. El factor para la elección, finalmente, ha sido mi propio interés personal. El desarrollo de la tecnología digital y el funcionamiento de las herramientas que resultan del mismo siempre han llamado mi atención y despertado mi curiosidad. La formación jurídica ha complementado esta fascinación, muchas veces aportando respuestas, pero otras veces generando más preguntas que quedaron sin respuesta.

La postura activa necesaria para llevar a cabo una investigación de cualquier tipo, es mucho mejor y dará mejores resultados si responde a estímulos intrínsecos. Trabajando con la nota informativa de derecho público, y luego con el debate, he podido comprobar los problemas para la calificación penal de los injustos cometidos con instrumentos de la prehistoria digital, incluso contando con una legislación perfectamente adaptada. Enseguida surgieron dudas: ¿Qué nos espera cuando todos podamos pagar y cobrar con el móvil? o ¿qué pasará cuando alguien pretenda denunciar una transferencia no consentida de bitcoins?

Pero elegir este tema también significaba un desafío. La información técnica relativa a los nuevos medios de pago es abundante, pero la literatura jurídica es prácticamente inexistente. Por un lado, el análisis de estos nuevos métodos resultaría seguramente motivante, pero por otro, la falta de apoyo doctrinal y teórico para darle al análisis mayor solidez desde el punto de vista jurídico me causaba un cierto vértigo. Además, los plazos previstos para la preparación y la redacción de este trabajo, así como los requisitos de validación del tema por el docente, no permitían una reflexión muy relajada.

El primer borrador de este trabajo se hizo en Río de Janeiro, donde tuve que desplazarme de manera imprevista por motivos personales. La situación no era la más propicia, pero allí pude contar con la ayuda de Pablo Serber para introducirme en los rudimentos de la criptografía y la seguridad informática de más alto nivel. Ya a la vuelta, me he visto trabajando en varios apartados a la vez sin hilo de continuidad en la redacción, lo que me ha llevado a cambiar completamente la estructura del trabajo para hacerlo más coherente, menos confuso y más explicativo. Adoptada la estructura ya definitiva, el trabajo de investigación pasó a ser casi un relato natural, gracias a lo cual pude dedicarme a él sin dejar de cumplir con todos los compromisos de estas fechas en L'Ametlla del Vallès y Valencia con mi familia, a la que agradezco su paciencia infinita.

REFERENCIAS BIBLIOGRÁFICAS

[1] **Banco Central Europeo** (2012). *Virtual currency schemes.* Frankfurt: Banco Central Europeo. [fecha de consulta: 22 de diciembre de 2015] <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

[2] **Carbonell Mateu, J.C.; Gili Pascual, A.; Llabrés Fuster, A. y Tomás-Valiente Lanuza, C**. (2015). *Introducción a la teoría del delito. La antijuridicidad (I). El hecho típico.* Barcelona: FUOC

[3] **Francis, L.; Hancke, G.; Mayes, K. y Markantonakis, K.** (2011). *Practical relay attack on contactless transactions by using NFC mobile phones.* [fecha de consulta: 23 de diciembre de 2015] <http://eprint.iacr.org/2011/618.pdf>

[4] **Maldonado, L.** (coord., 2015). *Los medios de pago, un paisaje en movimiento.* Madrid: Centro del Sector Financiero de PwC e IE Business School

[5] **Nakamoto, S.** (2008). *Bitcoin: a peer-to-peer electronic cash system.* [fecha de consulta: 20 de diciembre de 2015] <https://bitcoin.org/bitcoin.pdf>

[6] **National Institute of Standards and Technology** (2013). *Guidelines for managing the security of mobile devices in the enterprise.* [fecha de consulta: 22 de diciembre de 2015] <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>

[7] **Quintero Olivares, G.** (2012). *Defraudaciones e insolvencias punibles.* Barcelona: FUOC

[8] **Quintero Olivares, G.** (2012). *Falsedades.* Barcelona: FUOC

[9] **Robertshaw, S.** (ed.) (2015). *The collaborative economy. Impact and potential of collaborative Internet and additive manufacturing.* Bruselas: Unión Europea [fecha de consulta: 30 de diciembre de 2015] <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/547425/EPRS_STU%282015%29547425_EN.pdf>

[10] **Romero, P.** (2013, 1 de noviembre). "Así se incauta la Policía de bitcoins". *El Mundo.* Sección de tecnología [fecha de consulta: 26 de diciembre de 2015] <http://www.elmundo.es/tecnologia/2013/11/01/5270d45363fd3da7618b4576.html>

[11] **Soto Nieto, F.** (2005). *Utilización ilegítima de tarjetas de crédito. Robo con fuerza en las cosas. Nuevas consideraciones. Diario La Ley.* (nº 6252)

[12] *The rise and rise of bitcoin* [película cinematográfica] (2014). Nicholas Mross (dir. prod.). EE.UU. (96 min)

GLOSARIO

BTC bitcoin, como unidad de divisa.

CP Código Penal.

CP1973 Código Penal de 1973.

IVA impuesto sobre el valor añadido.

LO Ley Orgánica.

NFC *near field communication*, comunicación de campo cercano.

SEC *Securities and Exchange Commission*, agencia gubernamental de EE.UU.

STS sentencia del Tribunal Supremo.

SSTS sentencias del Tribunal Supremo.

TIC tecnologías de la información y la comunicación.

TJUE Tribunal de Justicia de la Unión Europea.

ANEXOS

Anexo I: STS, 2ª, de lo Penal, de 19 de abril de 1991

"(...) ***Primero.***
(...)
Para la consumación del delito de estafa del artículo 528 del C.P., se precisa, como elemento básico configurador, un engaño precedente o concurrente, espina dorsal, factor nuclear, alma y sustancia de la estafa, antes traducido en alguno de los ardides o artificios incorporados al listado de que el Código hacía mención, y hoy concebido con criterio de laxitud, sin recurrir a enunciados ejemplificativos, dada la ilimitada variedad de supuestos que la vida real ofrece, fruto del ingenio falaz y maquinador de los que tratan de aprovecharse del patrimonio ajeno.
Dicho engaño ha de ser «bastante», es decir, suficiente y proporcional para la consecución de los fines propuestos, cualquiera que sea su modalidad en la multiforme y cambiante operatividad en que se manifieste, habiendo de tener adecuada entidad para que en la convivencia social actúe como estímulo eficaz del traspaso patrimonial, debiendo valorarse aquella idoneidad tanto atendiendo a módulos objetivos como en función de las condiciones personales del sujeto afectado y de las circunstancias todas del caso concreto.
Tal engaño ha de mostrarse como originador o productor de un error esencial en el sujeto pasivo, desconocedor o con conocimiento deformado o inexacto de la realidad por causa de la falacia, mendacidad, fabulación o artificio que le antecede (...).
Como consecuencia de la insidiosa o mendaz actividad del agente se provoca una situación de error esencial, juicio falso determinante de un acto de disposición patrimonial por el sujeto pasivo, en íntimo nexo causal con la fingidora maquinación precedente.
Para que un determinado acto de disposición llegue a tener relevancia típica ha de ser inducido por el error causado y realizado, por lo tanto, por la víctima del ardid.
Segundo.
A la vista de ello, mal puede concluirse la perpetración de un delito de estafa por parte del procesado, al impedirlo la concepción legal y jurisprudencial del engaño, ardid que se produce e incide por y sobre personas, surgiendo en el afectado un vicio de voluntad por mor de la alteración psicológica provocada.
La «inducción» a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina, implica una dinámica comisiva con acusado substrato ideológico.
Con razón se ha destacado que a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa.
Sin engaño, elemento cardinal de la estafa, no puede entenderse producida ésta.
Tercero.
En relación con la consideración del hecho contemplado como constitutivo de un delito de apropiación indebida, ha de señalarse que tal fue la tesis de la defensa en la instancia, alternativa a la de la libre absolución, según se hace constar en el tercer antecedente de hecho de la sentencia recurrida.
En la exposición del motivo primero del recurso se vuelve a insistir en ello, aduciendo, tras rechazar la existencia de una inducción a otro a realizar un acto de disposición patrimonial, que existió auténtica disposición por parte del Sr. V.M., quien ostentaba la condición de apoderado - Banco Hispano Americano- de los fondos que le fueron entregados para su administración, elemento básico del tipo de apropiación indebida.
Siendo ello así, bien se deduce que el inculpado se apropió de dinero que tenía a su alcance por razón de su condición de apoderado de la entidad bancaria y en cuya administración tenía intervención directa, encaminándose los apuntes falsarios efectuados en el ordenador a justificar formalmente la disminución patrimonial de fondos derivada del hecho de la apropiación.

El supuesto ha de subsumirse en el tipo penal de la apropiación indebida.
(...)
Quinto.
Algunos delitos tipificados en el Código sustantivo admiten hoy su realización aun con instrumentos diferentes de los naturalmente concebibles al tiempo de su configuración legal, tales los medios informáticos, de generalizada e irreversible utilización, desplazando implacablemente los procedimientos manuales alternativos, hasta el extremo y con tal intensidad que difícilmente podrían sobrevivir muchas empresas sin que el auxilio de la técnica informática.
Esta viene apoyada sobre tres conceptos o manifestaciones que la configuran: grandes ordenadores que albergan una considerable información en forma de bases de datos, usuarios dispersos que, a través de redes de comunicaciones, acceden a aquélla, y ordenadores individuales que siguen trabajado y alimentando el ordenador central, como terminales del mismo.
Es en estos terminales donden pueden llevarse a efecto manipulaciones alteradoras de la verdad real, introduciendo movimientos falsos en todo o en parte o eliminando transacciones verdaderas que debieron ser introducidas, todo con correlativo reflejo e incorporación al soporte material magnético instalado en el ordenador central.
Los tradicionales instrumentos de contabilidad han sido traspasados a enunciados mecanismos informáticos, y, en última sede, al disco o soporte corpóreo asentado en el ordenador central.
Sus datos obtienen inmediata traducción legible en pantalla o se resuelven, merced a su instantánea impresión, en reproducción escrita en papel. (...) "

Anexo II: STS 257/2000, 2ª, de lo Penal, de 18 de febrero (rec. 504/1998)

*"(...)**TERCERO.** La expresión o denominación legal fuerza en las cosas aplicada a una de las especies del delito de robo constituye desde luego un concepto normativo no coincidente con su significado literal-gramatical o vulgar, debiendo necesariamente concurrir en los hechos para entender la existencia de fuerza, alternativamente, alguna de las circunstancias referidas en el artículo 238 CP, que constituye una enumeración cerrada, de forma que cualesquiera otra circunstancia no sería subsumible bajo la previsión legislativa del robo con fuerza en las cosas.*
Siendo ello así, el uso de llaves falsas, número 4º del artículo citado en último lugar, no implica el desarrollo de una especial fuerza o presión para acceder al lugar donde se encuentren las cosas muebles ajenas, sino el empleo de un medio que permita dicho acceso sin causar daños o desmedros, fundamentándose su autonomía frente al hurto, verdadero tipo básico contra la propiedad (artículo 234 C.P.), en circunstancias relativas tanto a la defensa desplegada por el propietario o poseedor legítimo de las cosas cuya sustracción se pretende como en la mayor astucia o habilidad del agente.
La Jurisprudencia de esta Sala sí puede afirmarse que ha consolidado un concepto jurídico relevante desde la perspectiva del delito de robo a lo largo del tiempo por lo que hace al entendimiento de la expresión normativa llave falsa que, a su vez, el propio legislador de 1.995 expresa en el hoy artículo 239 CP, antes 510, ampliando los supuestos de la consideración legal del instrumento referido.
Así, la STS 5 Nov. 1987, se refiere en relación al antiguo 504.4, «uso de llaves falsas, ganzúas u otros instrumentos semejantes», a haber sido interpretado por la doctrina de esta Sala «en el sentido de que el empleo de cualquier instrumento, distinto de la llave legítima, que resulte idóneo para abrir una puerta cerrada, se constituye en medio de fuerza que convierte en delito de robo la sustracción de la cosa mueble ajena, lo que quiere decir que la semejanza exigible entre las llaves falsas y ganzúas y cualquier otro instrumento es de índole meramente funcional y no morfológico», bastando que el instrumento en la práctica sea apto para accionar un mecanismo de cierre de una puerta dejando abierto y expedito lo que previamente estaba cerrado. Las SSTS 6 Mar. 1989 y 27 Feb. 1990, inciden en que el concepto de llaves falsas no se corresponde con el significado vulgar y usual de la misma sino que es eminentemente funcional. La STS 20 Sep. 1990, tratándose del supuesto tan debatido en su momento de las tarjetas bancarias o de crédito, incide en lo anterior, haciendo especial hincapié en que dicha

funcionalidad, que permite entender como llaves las referidas tarjetas, lo que «no agravia el principio de legalidad porque no existe una extensión analógica de «llave» superadora del artículo 25 CE, sino una simple aplicación analógica expresamente autorizada en el Texto penal bajo la fórmula legal de enumerar o mencionar previamente algunos medios concretos, de suerte que el juicio de semejanza o analogía no queda entregado a la libre valoración del Tribunal», lo que es relevante como después veremos. La de 8 May. 1992 que se ocupa extensamente de la cuestión en relación también especialmente con las tarjetas y la doble función de las mismas como llaves en sentido estricto que permiten acceder al continente donde se ubica el cajero y como instrumento que activa el funcionamiento de este último. También la 24 Abr. 1996, y, por último, la de 16 Mar. 1999 que compendia la anterior doctrina al respecto también en un caso de tarjetas magnéticas, afirmando, a los efectos del delito de robo, «que la llave no tiene que ser un instrumento metálico o compuesto de un material determinado, como dice la definición primera que nos ofrece al respecto el Diccionario de la Real Academia de la Lengua Española, pudiendo ser de cualquier material y cualquiera que sea el mecanismo de apertura o cierre, exigiéndose simplemente que sirva para abrir o cerrar tal mecanismo sin producir rotura, con cuya utilización conforme a su propio destino se logra acceder al lugar o al interior del objeto donde se encuentra la cosa mueble que se sustrae». Después de la entrada en vigor del CP 1995, el último párrafo del nuevo artículo 239 equipara a llaves por asimilación legal las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

(...)

***QUINTO**. El nuevo artículo 237, frente al 500 del Código de 1973, añade la expresión, cuando se trata de robo con fuerza en las cosas, «para acceder al lugar donde éstas se encuentran», y ello significa que indistintamente el delito se comete empleando el instrumento como medio de acceso al continente o lugar mediato donde se encuentran las cosas muebles ajenas, en el presente caso la máquina expendedora, o bien al concreto receptáculo comprendido en dicho continente provisto de su propio mecanismo de seguridad o cierre, que es lo que sucede en el presente caso. Ello tampoco constituye ninguna novedad si tenemos en cuenta la doble función de las tarjetas de crédito a que ya hemos hecho referencia más arriba y el entendimiento de la comisión del delito de robo tanto en un caso, acceso al lugar donde se encuentra el cajero, como en otro, apertura del mecanismo de funcionamiento del propio cajero, analogía evidente puesto que es indiferente que el sistema de apertura sea mecánico o electrónico. En síntesis, lo esencial es la posibilidad de liberar un mecanismo cerrado en principio que preserva el depósito y libre disposición de los bienes muebles de que se trate, sin que ello signifique la necesidad de la previa apertura de la caja o mueble donde dicho mecanismo está alojado, mediante la utilización de un artificio o instrumento que funcionalmente sea idóneo para ello, quebrantando de esta forma el dispositivo de seguridad establecido. (...)"*

Anexo III: STS 2016/2000, 2ª, de lo Penal, de 26 de diciembre (rec. 254/1999)

*"(...) **Recurso del Ministerio Fiscal** En el primer motivo que interpone el Ministerio fiscal denuncia el error de derecho producido en la sentencia al inaplicar, al hecho probado, los arts. 237, 238.4 y 239.2 y último párrafo del Código Penal argumentando que el relato fáctico, al declarar probado la sustracción de dinero en los cajeros automáticos que relata, ha de subsumirse en el delito de robo con fuerza en las cosas y no en el delito de estafa que ha aplicado el tribunal de instancia.*

El motivo debe ser estimado. Es reiterada la jurisprudencia de esta Sala, anterior y posterior a la entrada en vigor de Código Penal de 1995, que subsume en el delito de robo con fuerza en las cosas los apoderamientos de dinero utilizando tarjetas de crédito de las que se conoce el número secreto que permite el acceso a los fondos depositados. (Cfr. TS SS 1658/1998, de 17 Dic., 427/1999, de 16 Mar. y 666/1999, de 29 Abr.). La jurisprudencia de esta Sala ha declarado que el apoderamiento dinerario a través de la introducción en el cajero automático de una entidad bancaria, cualquiera que sea el lugar de su ubicación conociéndose el número secreto constituye un delito de robo fuera ya de su conexión con la sustracción inicial de la

tarjeta, porque tiene lugar el apoderamiento de una cosa mueble sin la voluntad de su dueño mediante el uso de una llave falsa, dado que la tarjeta magnética obtenida según se declara probado tiene la consideración de llave falsa.
La pretendida colisión de normas que se argumenta en la fundamentación de la sentencia, entre los artículos que tipifican el delito de robo con fuerza en las cosas y la estafa del art. 248.2 tipificador de la estafa, no existe. El art. 248.2 del código exige en su redacción la realización de actos de manipulación informática o artificio semejante, elemento de la acción que no concurre cuando lo que se realiza es un apoderamiento de dinero mediante el empleo de una tarjeta válida y el número secreto correspondiente, sin ninguna manipulación informática sino el empleo de una llave, art. 239 último párrafo, sustraída a su titular.
(...)
En el caso de autos, cada una de las operaciones en las que Jeany Ives B. L. (lo que se reproduce para el condenado en la sentencia que se recurre toda vez que intervino en la acción) imitó la firma de Dolores F. S. en los talones de compra de distintas prendas de vestir, en el establecimiento de «Gonzalo Comella», fingiendo al mismo tiempo ser la titular de la tarjeta de crédito de Dolores que había hurtado, era subsumible en el tipo de falsedad documental cometida por particulares, previsto en el art. 390.3º en relación con el 392 CP de 1995, en cuanto que la acusada en la firma de cada taloncillo de compra supuso la intervención de una persona --Dolores F. S.-- que no había intervenido y le atribuyó unas manifestaciones de voluntad relativas a la compra de las prendas relacionadas en cada taloncillo y al pago a través de la cuenta de la red 6000 de «Caixa de Manlleu que Dolores no había hecho.
La firma de cada taloncillo de compra constituyó un documento distinto, y una acción falsaria independiente. Hubo pluralidad de acciones, ya que hubo solución de continuidad separadora de las estampaciones de la firma en cada documento.
El hecho de que todos ellos dimanasen de la misma operación de compra, no hace perder su individualidad e identidad delictiva a cada una de las acciones falsarias, sino que, según lo argumentado por el Ministerio Fiscal, determinó la continuidad de las mismas, por imperativo de lo dispuesto en el art. 74, ap. 1 CP de 1995. Efectivamente, se dieron de forma cumplida en el supuesto de autos las condiciones de la continuidad delictiva que el precepto citado establece, y que la jurisprudencia ha señalado, pues las acciones falsarias obedecieron a un unitario propósito criminal, se realizaron aprovechando idéntica ocasión, supusieron la infracción del mismo precepto penal, y concurrieron respecto a ellas los requisitos de la proximidad temporal, que fue casi simultaneidad de la coincidencia local y de la identidad de método delictivo.
(...)
***Fallamos**: Que debemos condenar y condenamos al acusado, Juan Mª E. N., como autor de un delito continuado de falsedad en documento mercantil, cometido por particulares, en concurso medial con un delito continuado de estafa, y sin circunstancias genéricas modificativas de la responsabilidad penal, a la pena de 2 años y 4 meses y 15 días de prisión y multa de 9 meses con cuota diaria de 1.000 ptas., que deberá satisfacer en nueve plazos mensuales de 30.000 ptas. cada uno de ellos, y en los 15 primeros días de cada mes a contar desde la firmeza de la presente resolución, y con 3 meses de responsabilidad subsidiaria en caso de impago; como autor de un delito de robo con fuerza en las cosas a la pena de 1 año de prisión; como autor de una falta de hurto a la pena de un mes de multa con una cuota diaria de 1.000 ptas. con 15 días de responsabilidad personal subsidiaria en caso de insolvencia. Asimismo, el pago de la mitad de las costas procesales. Así como a que, en concepto de responsabilidad civil indemnice, de forma conjunta y solidaria con la ya condenada en esta causa en la sentencia de fecha 5 Abr. 1998, a Dolores F. S. en la cantidad de 1.000 ptas."*

Anexo IV: STS 369/2007, 2ª, de lo Penal, de 9 de mayo (rec. 11142/2006)

"(...)Del mismo modo resultaría absurdo que en casos de uso de las tarjetas originales o clonadas, tanto en cajeros como también en establecimientos comerciales, se sumaran los delitos de robo y de estafa, en la medida de que el animo de lucro se agota en un propósito continuado único, y en el relato fáctico expresamente se dice que el acusado junto con otros

individuos que no han podido ser identificados hasta la fecha, formaban un grupo dedicado a la clonación de tarjetas de crédito y "su utilización fraudulenta con fines lucrativos", y a continuación se describe los dos procedimientos utilizados por el acusado: "skimming" para clonar tarjetas cuyo "fin ultimo de tales tarjetas falsificadas era realizar compras en establecimientos comerciales, utilizando al efecto la documentación alterada oportuna para identificarse como el titular de la tarjeta, y también para extraer dinero en cajeros de entidades de crédito", y el procedimiento de "siembra" en cuyo caso "las tarjetas obtenidas con tal procedimiento son utilizadas para extraer dinero de los cajeros". Y al acusado se le ocuparon tarjetas obtenidas mediante ambas modalidades, indicándose en el factum que los perjuicios acreditados mediante las tarjetas intervenidas lo fueron mediante el uso de las tarjetas en los cajeros.

Por ello si de desdobla la calificación jurídica del uso de la tarjeta de modo que su uso en local comercial es constitutivo de estafa, pues se acepta doctrinal y jurisprudencialmente que la persona que habiéndose hecho con una tarjeta de la que no es titular, finge serlo en una operación presencial, consiguiendo de este modo, que el establecimiento le proporcione bienes o servicios, consuma un delito de estafa, pues provoca, presentando la tarjeta, una apariencia de crédito o de garantía de pago de la que realmente carece y provoca, de este modo, una disposición que ha de ser asumido por una persona jurídica que se comprometió a ello bajo presuposición de normalidad de uso, y su utilización en cajero es merecedor de la calificación de robo, nos hallaríamos ante dos delitos distintos en concurso, un robo con fuerza en las cosas en relación a los cajeros, y un delito de estafa en cuanto a su uso en establecimientos comerciales -en los hechos probados, apartado cuarto se recoge como las tarjetas regalo de El Corte Ingles sirvieron para el clonado de diversas tarjetas, realizándose con siete de ellas operaciones ilícitas- y resultaría absurda y más grave para el acusado esta separación en dos delitos de lo que no es sino una única intención y manifestación delictiva de obtener metálico o efectos mediante las tarjetas, que merece la única respuesta punitiva de la estafa. (...)"

Anexo V: *Consumers and mobile financial services 2015*, Reserva Federal

Encuesta sobre el uso de pagos con dispositivos móviles:

Tabla C.39. Al realizar pagos con dispositivos móviles ¿Cuál de los siguientes métodos de pago utiliza?	
NC	2,0%
Tarjeta de crédito	51,2%
Tarjeta de débito	55,0%
Tarjeta de débito prepago	7,6%
Cuenta bancaria	40,7%
Cuenta no bancaria (ej.: PayPal)	15,4%
Otro	3,1%
Número de respuestas válidas	455